# 日本国特許庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１２月　３日

出願番号
Application Number: 特願２００２－３５１０６３

[ST. 10/C]: [ＪＰ２００２－３５１０６３]

出願人
Applicant(s): 松下電器産業株式会社

２００３年１１月　４日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０９１０８８

【書類名】　特許願
【整理番号】　2022540497
【提出日】　平成14年12月 3日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/32
G09C 1/00 640
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　山道　将人
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　布田　裕一
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　大森　基司
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　館林　誠
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100097445
【弁理士】
【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　暗号システム、暗号装置、復号装置、共有鍵生成装置及び共有鍵復元装置

【特許請求の範囲】

【請求項１】　共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、

秘密数データを生成する秘密数データ生成手段と、

前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出手段と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して暗号化共有鍵データを生成する第１の暗号化手段とを備えることを特徴とする、共有鍵生成装置。

【請求項２】　共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、

秘密数データを生成する秘密数データ生成手段と、

前記秘密数データを所定の処理に基づいて検証値データと乱数データと前記共有鍵データに変換する共有鍵導出手段と、

前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化手段と、

前記秘密数データを前記検証値データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化手段とを備え、

前記暗号化共有鍵データは、前記第１の暗号予備データと前記第２の暗号予備データから構成されることを特徴とする、共有鍵生成装置。

【請求項３】　前記第２の暗号化手段は、前記秘密数データと前記検証値データの排他的論理和演算を行って前記第２の暗号予備データを生成することを特徴とする、請求項２に記載の共有鍵生成装置。

【請求項４】　前記第２の暗号化手段は、前記秘密数データを、前記検証値デ

ータを暗号鍵として用いて共通鍵暗号方式により暗号化して前記第２の暗号予備データを生成することを特徴とする、請求項２に記載の共有鍵生成装置。

【請求項５】　前記第２の暗号化手段は、前記秘密数データに前記検証値データを加算して前記第２の暗号予備データを生成することを特徴とする、請求項２に記載の共有鍵生成装置。

【請求項６】　前記第２の暗号化手段は、前記秘密数データに前記検証値データを乗算して前記第２の暗号予備データを生成することを特徴とする、請求項２に記載の共有鍵生成装置。

【請求項７】　前記暗号化共有鍵データは、前記第１の暗号予備データと前記第２暗号予備データのビット連結データであることを特徴とする、請求項２から請求項６のいずれか一項に記載の共有鍵生成装置。

【請求項８】　前記第１の暗号化手段は、ＮＴＲＵ暗号方式により暗号化して前記暗号化共有鍵データを生成することを特徴とする、請求項１に記載の共有鍵生成装置。

【請求項９】　前記第１の暗号化手段は、ＮＴＲＵ暗号方式により暗号化して前記第１の暗号予備データを生成することを特徴とする、請求項２から請求項７のいずれか一項に記載の共有鍵生成装置。

【請求項１０】　前記秘密数データは、ランダムに生成される乱数であることを特徴とする、請求項１から請求項９のいずれか一項に記載の共有鍵生成装置。

【請求項１１】　前記共有鍵導出手段は、所定の処理として、一方向性ハッシュ関数を用いることを特徴とする、請求項１から請求項１０のいずれか一項に記載の共有鍵生成装置。

【請求項１２】　予め与えられた秘密鍵データ及び公開鍵データに基づいて、暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、

前記暗号化共有鍵データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第１の復号化手段と、

前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出手段と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して再暗号化共有鍵データを生成する第３の暗号化手段とを備え、

前記暗号化共有鍵データと前記再暗号化共有鍵データが一致する場合に、前記共有鍵データを出力することを特徴とする、共有鍵復元装置。

【請求項１３】　予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、

前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化手段と、

前記第２の暗号予備データを前記検証値データに基づいて復号化して秘密数データを生成する第２の復号化手段と、

前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出手段と、

前記検証値検証データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化手段とを備え、

前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記共有鍵データを出力することを特徴とする、共有鍵復元装置。

【請求項１４】　予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、

前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化手段と、

前記第２の暗号予備データを前記検証値データに基づいて復号化して秘密数データを生成する第２の復号化手段と、

前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出手段と、

前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化手段とを備え、

前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前

記共有鍵データを出力することを特徴とする、共有鍵復元装置。

【請求項１５】　前記第２の復号化手段は、前記第２の暗号予備データと前記検証値データの排他的論理和演算を行って前記秘密数データを生成することを特徴とする、請求項１３または請求項１４に記載の共有鍵復元装置。

【請求項１６】　前記第２の復号化手段は、前記第２の暗号予備データを、前記検証値データを暗号鍵として用いて共通鍵暗号方式により復号化して前記秘密数データを生成することを特徴とする、請求項１３または請求項１４に記載の共有鍵復元装置。

【請求項１７】　前記第２の復号化手段は、前記第２の暗号予備データに前記検証値データを減算して前記秘密数データを生成することを特徴とする、請求項１３または請求項１４に記載の共有鍵復元装置。

【請求項１８】　前記第２の暗号化手段は、前記第２の暗号予備データを前記検証値データで除算して前記秘密数データ第２の秘密数データを生成することを特徴とする、請求項１３または請求項１４に記載の共有鍵復元装置。

【請求項１９】　前記第１の復号化手段は、ＮＴＲＵ暗号方式により復号化して前記共有鍵データを生成することを特徴とする、請求項１２に記載の共有鍵復元装置。

【請求項２０】　前記第１の復号化手段は、ＮＴＲＵ暗号方式により復号化して前記検証値データを生成することを特徴とする、請求項１３から請求項１８のいずれか一項に記載の共有鍵復元装置。

【請求項２１】　前記共有鍵導出手段は、所定の処理として、一方向性ハッシュ関数を用いることを特徴とする、請求項１５から請求項２０のいずれか一項に記載の共有鍵復元装置。

【請求項２２】　予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置であって、

秘密数データを生成する秘密数データ生成手段と、

前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して

第１の暗号予備データを生成する第１の暗号化手段と、

前記平文データを前記共有鍵データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化手段とを備え、

前記暗号文データは、前記第１の暗号予備データと前記第２の暗号予備データから構成されることを特徴とする、暗号装置。

【請求項２３】　予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号文データを復号して復号文データを出力する復号装置であって、

前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第１の復号化手段と、

前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化手段とを備え、

前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記第２の暗号予備データを前記共有鍵に基づいて復号化して前記復号文データを生成する復号手段とを備えることを特徴とする、復号装置。

【請求項２４】　予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置、及び予め与えられた秘密鍵データ及び公開鍵データに基づいて暗号文データを復号して復号文データを出力する復号装置からなる暗号システムであって、

前記暗号装置は、

秘密数データを生成する秘密数データ生成手段と、

前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化手段と、

前記平文データを前記共有鍵データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化手段とを備え、

前記暗号文データは、前記第１の暗号予備データと前記第２の暗号予備データと前記第３の暗号予備データから構成され、

前記復号装置は、

前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第１の復号化手段と、

前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化手段とを備え、

前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記第２の暗号予備データを前記共有鍵に基づいて復号化して前記復号文データを生成する復号手段とを備えることを特徴とする、暗号システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報セキュリティ技術としての暗号技術に関し、特に、公開鍵暗号を用いた鍵配送に関するものである。

【０００２】

【従来の技術】

送信装置と受信装置との間で秘匿通信を実現する方法として、公開鍵暗号を用いた暗号化通信がある。簡単に説明すると、送信装置が、通信内容を受信装置の公開鍵を用いて暗号化して送信し、受信装置は、暗号化された通信内容を受信し、それを自身の秘密鍵を用いて復号して元の通信内容を得る方法である（例えば、非特許文献１参照。）。この方法を用いる一般的な暗号システムでは、送信装置及び受信装置は、ともに複数存在する。まず、送信装置は、通信先受信装置の公開鍵を取得する。この公開鍵は、通信先受信装置が有する秘密鍵と対になるものでありシステムにおいて公開されている。そして、送信装置は、通信すべきデータ内容を上記のように取得した公開鍵で暗号化して送信する。一方で、受信装置は、上記のように暗号化された通信内容データを受信する。そして、受信装置

は、暗号化された通信内容データを、自身の有する秘密鍵で復号して元の通信内容データを得る。

【０００３】

１９９６年、高速処理が可能な公開鍵暗号として、ＮＴＲＵ暗号が提案された（例えば、非特許文献２参照。）。このＮＴＲＵ暗号については、非特許文献２に詳細が記載されているのでここでは詳細な説明を省略するが、べき乗演算を行うＲＳＡ暗号や楕円曲線上の点のスカラ倍演算を行う楕円曲線暗号に比べ、高速に演算可能な多項式演算で暗号化と復号化を行うので、従来の公開鍵暗号よりもソフトウェアにより高速に処理することが可能である。なお、このＮＴＲＵ暗号方式は、公開鍵を用いて平文を暗号化して暗号文を生成し、正規の秘密鍵を用いて暗号文を復号して復号文を生成しても、復号文が元の平文と異なる場合が発生する。このことを復号エラーが発生するという。なお、復号エラーを回避する方法として、平文に付加情報を付加して暗号化し、平文のハッシュ関数値と共に送信する方法が開示されている（例えば、特許文献１参照。）。

【０００４】

一方で、近年、公開鍵暗号の新しい概念として、鍵カプセル化メカニズム（Ｋｅｙ　Ｅｎｃａｐｓｕｌａｔｉｏｎ　Ｍｅｃｈａｎｉｓｍｓ）と呼ばれる方式が提案された（例えば、非特許文献３参照。）。この鍵カプセル化メカニズムは、簡単に説明すると、公開鍵暗号を用いて送信装置と受信装置の間で共有鍵を配送するアルゴリズムであり、送信側が、暗号化アルゴリズムＥに受信者の公開鍵ｐｋを入力して暗号文Ｃと共有鍵Ｋを生成し、暗号文Ｃを受信側に伝送する。そして、受信側が、復号アルゴリズムＤに、秘密鍵ｓｋと暗号文Ｃを入力して送信側と同じ共有鍵Ｋを求める方式である。この鍵カプセル化メカニズムの目的は、鍵カプセル化メカニズムで共有鍵Ｋを送信装置と受信装置で共有することにより、その後、送信装置から受信装置へ通信される通信内容データを、共有鍵Ｋを用いて共通鍵暗号で暗号化することにある。ここで、送信者から受信者に一方的に情報の送信が行われていながら、送信者が作為的に共有鍵を作成できず、送信者による不正が抑制されている点が従来にない特長である。

【０００５】

このような鍵カプセル化メカニズムとして、ＲＳＡ－ＫＥＭと呼ばれるアルゴリズムが開示されている（例えば、非特許文献３参照。）。以下に、この非特許文献３に記載されているＲＳＡ－ＫＥＭアルゴリズムについて説明する。

【０００６】

（１）ＲＳＡ－ＫＥＭのシステムパラメータ

ＲＳＡ－ＫＥＭは、以下のシステムパラメータを持つ。

【０００７】

・ハッシュ関数：Ｇ

なお、ハッシュ関数については、非特許文献１に詳細が記述されているので、ここでは説明を省略する。

【０００８】

（２）ＲＳＡ－ＫＥＭの公開鍵と秘密鍵

・素数ｐ、ｑを選び、ｎ＝ｐ・ｑを生成する。

【０００９】

・（ｐ－１）と（ｑ－１）の最小公倍数を計算し、Ｌとする。

【００１０】

・ランダムに、Ｌと互いに素であるＺＬの要素ｅを選び、ｄ＝１／ｅ　ｍｏｄ　Ｌを計算する。

【００１１】

ここで、ＺＬは、｛０，１，２，．．．，Ｌ－１｝からなる集合である。

【００１２】

・公開鍵ｐｋを（ｅ，ｎ）とし、秘密鍵ｓｋを（ｄ，ｎ）とする。

【００１３】

（３）ＲＳＡ－ＫＥＭの暗号化

暗号化時には、以下に述べる暗号化アルゴリズムＫｅｍＥに公開鍵ｐｋを入力して共有鍵Ｋと暗号文Ｃを出力する。以下に暗号化アルゴリズムＫｅｍＥについて説明する。

【００１４】

・Ｚｎの要素ｓをランダムに生成する。

【００１５】

ここで、Ｚｎは、｛０，１，２，．．．，ｎ－１｝からなる集合である。

【００１６】

・Ｇ（ｓ）を生成し、Ｋ＝Ｇ（ｓ）とする。

【００１７】

・Ｃ＝ｓ＾ｅ　ｍｏｄ　ｎを生成する。ここで「＾」はべき乗を表す。

【００１８】

・共有鍵Ｋと暗号文Ｃを出力する。

【００１９】

（４）ＰＳＥＣ－ＫＥＭの復号化

復号化時には、以下に述べる復号アルゴリズムＫｅｍＤに暗号文Ｃと秘密鍵ｓｋを入力して共有鍵Ｋを出力する。以下に復号アルゴリズムＫｅｍＤについて説明する。

【００２０】

・ｓ＝Ｃ＾ｄ　ｍｏｄ　ｎを生成する。

【００２１】

・Ｇ（ｓ）を生成し、Ｋ＝Ｇ（ｓ）とする。

【００２２】

・共有鍵Ｋを出力する。

【００２３】

このＲＳＡ－ＫＥＭアルゴリズムを、送信装置と受信装置の間で暗号化通信を行う暗号システムに応用した場合、まず、送信装置は、通信先受信装置の公開鍵ｐｋを取得し、取得した公開鍵ｐｋを前述の暗号化アルゴリズムＫｅｍＥに入力して共有鍵Ｋと暗号文Ｃを導出して、暗号文Ｃを受信装置へ送信する。そして、受信装置は、送信装置から暗号文Ｃを受信し、受信した暗号文Ｃと自身が有する秘密鍵ｓｋを前述の復号アルゴリズムＫｅｍＤに入力して、送信装置が導出したものと等しい共有鍵Ｋを導出する。

【００２４】

以下に、このことを詳細に説明する。

【００２５】

今、ＲＳＡ－ＫＥＭアルゴリズムは、暗号化アルゴリズムＫｅｍＥで、ランダムに生成した要素ｓを公開鍵ｐｋを用いて暗号化して暗号文Ｃを生成する。そして、復号アルゴリズムＫｅｍＤでは、暗号文Ｃから秘密鍵ｓｋを用いて復号化して、暗号化アルゴリズムＫｅｍＥにおいて生成されたランダムな要素ｓを求めることができる。従って、暗号化アルゴリズムＫｅｍＥと復号アルゴリズムＫｅｍＤは、ハッシュ関数Ｇに同じｓの値を入力することができ、同じ共有鍵Ｋを導出することができる。この結果、秘密鍵ｓｋを有する受信装置は、送信装置が導出したものと同じ共有鍵Ｋを導出できることになる。

【００２６】

一方で、秘密鍵ｓｋを知らない他の受信装置は、たとえ公開鍵ｐｋを取得して暗号文Ｃを受信したとしても、秘密鍵ｓｋを知らないのでＣからｓを求めることができず、送信装置が導出したものと同じ共有鍵Ｋを導出できない。

【００２７】

よって、以上により、送信装置と受信装置とは、共有鍵Ｋを秘密に共有することができ、この後、秘密鍵暗号を用いて、送信装置から受信装置へ通信される通信内容データを、共有鍵Ｋを用いて共通鍵暗号で暗号化することができる。

【００２８】

【特許文献１】

特開２００２－２５２６１１号公報

【非特許文献１】

岡本龍明、山本博資、「現代暗号」、シリーズ／情報科学の数学、産業図書、1997.

【非特許文献２】

Jeffery Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp.267-288, Springer-Verlag, 1998.

【非特許文献３】

Victor Shoup, "A proposal for an ISO standard for public k

ey encryption (version 2.1)"、[online]、2001年12月20日、[2002年9月29日検索]、インターネット<URL: http://shoup.net/papers/iso-2_1.pdf>

【００２９】

【発明が解決しようとする課題】

上述したように、ＲＳＡ－ＫＥＭアルゴリズムは、暗号文Ｃから秘密鍵を知らなければ導出できないランダムな要素ｓをハッシュ関数Ｇに入力して共有鍵Ｋを導出するようにしている。従って、秘密鍵を知らなければその共有鍵Ｋを導出できないようにしている。

【００３０】

しかしながら、ＮＴＲＵ暗号は、鍵カプセル化メカニズムであるＲＳＡ－ＫＥＭアルゴリズムを適用して共有鍵の配送を行おうとすると、復号エラーが発生した場合、秘密鍵を用いてもランダムな要素ｓが正しく導出できないので、正しい共有鍵Ｋを導出ないという問題点がある。すなわち、高速処理が可能なＮＴＲＵ暗号は、鍵カプセル化メカニズムであるＲＳＡ－ＫＥＭアルゴリズムを適用しても、送信装置と受信装置との間で異なる鍵が導出される場合があり、従って、鍵カプセル化メカニズムにより導出される鍵を用いた送信装置から受信装置への確実な暗号化通信ができない。

【００３１】

また、特許文献１は、暗号における復号エラー発生検出技術であり、鍵カプセル化メカニズムについては言及されていない。

【００３２】

そこで、本発明は上記の課題に鑑み、ＮＴＲＵ暗号を用いて新しい鍵カプセル化メカニズムを構成し、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できる暗号システム、暗号装置、復号装置を提供することを第１の目的とする。

【００３３】

また、他の公開鍵暗号を用いて新しい鍵カプセル化メカニズムを構成し、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できる暗号システム、暗号装置、復号装置を提供することを第２の目的とする。

【００３４】

【課題を解決するための手段】

請求項１における発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成手段と、前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して暗号化共有鍵データを生成する第１の暗号化手段とを備えることを特徴とする。

【００３５】

請求項２における発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成手段と、前記秘密数データを所定の処理に基づいて検証値データと乱数データと前記共有鍵データに変換する共有鍵導出手段と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化手段と、前記秘密数データを前記検証値データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化手段とを備え、前記暗号化共有鍵データは、前記第１の暗号予備データと前記第２の暗号予備データから構成されることを特徴とする。

【００３６】

請求項３における発明は、請求項２に記載の共有鍵生成装置は、前記第２の暗号化手段が、前記秘密数データと前記検証値データの排他的論理和演算を行って前記第２の暗号予備データを生成することを特徴とする。

【００３７】

請求項４における発明は、請求項２に記載の共有鍵生成装置は、前記第２の暗号化手段が、前記秘密数データを、前記検証値データを暗号鍵として用いて共通鍵暗号方式により暗号化して前記第２の暗号予備データを生成することを特徴とする。

【００３８】

請求項５における発明は、請求項２に記載の共有鍵生成装置は、前記第２の暗号化手段が、前記秘密数データに前記検証値データを加算して前記第２の暗号予備データを生成することを特徴とする。

【００３９】

請求項６における発明は、請求項２に記載の共有鍵生成装置は、前記第２の暗号化手段が、前記秘密数データに前記検証値データを乗算して前記第２の暗号予備データを生成することを特徴とする。

【００４０】

請求項７における発明は、請求項２から請求項６のいずれか一項に記載の共有鍵生成装置は、前記暗号化共有鍵データが、前記第１の暗号予備データと前記第２暗号予備データのビット連結データであることを特徴とする。

【００４１】

請求項８における発明は、請求項１に記載の共有鍵生成装置は、前記第１の暗号化手段が、ＮＴＲＵ暗号方式により暗号化して前記暗号化共有鍵データを生成することを特徴とする。

【００４２】

請求項９における発明は、請求項２から請求項７のいずれか一項に記載の共有鍵生成装置は、前記第１の暗号化手段が、ＮＴＲＵ暗号方式により暗号化して前記第１の暗号予備データを生成することを特徴とする。

【００４３】

請求項１０における発明は、請求項１から請求項９のいずれか一項に記載の共有鍵生成装置は、前記秘密数データが、ランダムに生成される乱数であることを特徴とする。

【００４４】

請求項１１における発明は、請求項１から請求項１０のいずれか一項に記載の共有鍵生成装置は、前記共有鍵導出手段が、所定の処理として、一方向性ハッシュ関数を用いることを特徴とする。

【００４５】

請求項１２における発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記暗号化共有鍵データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第１の復号化手段と、前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して再暗号化共有鍵データを生成する第３の暗号化手段とを備え、前記暗号化共有鍵データと前記再暗号化共有鍵データが一致する場合に、前記共有鍵データを出力することを特徴とする。

【００４６】

請求項１３における発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化手段と、前記第２の暗号予備データを前記検証値データに基づいて復号化して秘密数データを生成する第２の復号化手段と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出手段と、前記検証値検証データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化手段とを備え、前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記共有鍵データを出力することを特徴とする。

【００４７】

請求項１４における発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化手段と、前記第２の暗号予備データを前記検証値データに基づいて復号化して秘密数データを生成する第２の復号化手段と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データ

に変換する共有鍵導出手段と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化手段とを備え、前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記共有鍵データを出力することを特徴とする。

【００４８】

請求項１５における発明は、請求項１３または請求項１４に記載の共有鍵復元装置は、前記第２の復号化手段が、前記第２の暗号予備データと前記検証値データの排他的論理和演算を行って前記秘密数データを生成することを特徴とする。

【００４９】

請求項１６における発明は、請求項１３または請求項１４に記載の共有鍵復元装置は、前記第２の復号化手段が、前記第２の暗号予備データを、前記検証値データを暗号鍵として用いて共通鍵暗号方式により復号化して前記秘密数データを生成することを特徴とする。

【００５０】

請求項１７における発明は、請求項１３または請求項１４に記載の共有鍵復元装置は、前記第２の復号化手段が、前記第２の暗号予備データに前記検証値データを減算して前記秘密数データを生成することを特徴とする。

【００５１】

請求項１８における発明は、請求項１３または請求項１４に記載の共有鍵復元装置は、前記第２の暗号化手段が、前記第２の暗号予備データを前記検証値データで除算して前記秘密数データ第２の秘密数データを生成することを特徴とする。

【００５２】

請求項１９における発明は、請求項１２に記載の共有鍵復元装置は、前記第１の復号化手段が、ＮＴＲＵ暗号方式により復号化して前記共有鍵データを生成することを特徴とする。

【００５３】

請求項２０における発明は、請求項１３から請求項１８のいずれか一項に記載の共有鍵復元装置は、前記第１の復号化手段が、ＮＴＲＵ暗号方式により復号化

して前記検証値データを生成することを特徴とする。

【００５４】

請求項２１における発明は、請求項１５から請求項２０のいずれか一項に記載の共有鍵復元装置は、前記共有鍵導出手段が、所定の処理として、一方向性ハッシュ関数を用いることを特徴とする。

【００５５】

請求項２２における発明は、予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置であって、秘密数データを生成する秘密数データ生成手段と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化手段と、記平文データを前記共有鍵データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化手段とを備え、前記暗号文データは、前記第１の暗号予備データと前記第２の暗号予備データから構成されることを特徴とする。

【００５６】

請求項２３における発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号文データを復号して復号文データを出力する復号装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第１の復号化手段と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化手段とを備え、前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記第２の暗号予備データを前記共有鍵に基づいて復号化して前記復号文データを生成する復号手段とを備えることを特徴とする。

【００５７】

請求項２４における発明は、予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置、及び予め与えられた秘密鍵デ

ータ及び公開鍵データに基づいて暗号文データを復号して復号文データを出力する復号装置からなる暗号システムであって、前記暗号装置は、秘密数データを生成する秘密数データ生成手段と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化手段と、前記平文データを前記共有鍵データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化手段とを備え、前記暗号文データは、前記第１の暗号予備データと前記第２の暗号予備データと前記第３の暗号予備データから構成され、前記復号装置は、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第１の復号化手段と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化手段とを備え、前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記第２の暗号予備データを前記共有鍵に基づいて復号化して前記復号文データを生成する復号手段とを備えることを特徴とする。

【００５８】

【発明の実施の形態】

以下、本発明に係る暗号システムの実施の形態について、図面を用いて説明する。

【００５９】

本発明に係る暗号システムは、公開鍵暗号方式の一例として、ＮＴＲＵ暗号方式を用いる。ＮＴＲＵ暗号方式は、多項式の演算で暗号化と復号化を行う公開鍵暗号方式である。このＮＴＲＵ暗号方式、及びＮＴＲＵ暗号方式の公開鍵、及び秘密鍵の生成方法については、非特許文献２に詳しく述べられているので、ここでは詳細な説明を省略するが、以下にＮＴＲＵ暗号方式について簡単に説明する。

【００６０】

（１）ＮＴＲＵ暗号方式のシステムパラメータ

ＮＴＲＵ暗号方式は、整数のシステムパラメータ、Ｎ、ｐ、ｑを持つ。上記文献には、システムパラメータの例として、（Ｎ，ｐ，ｑ）＝（１０７，３，６４）、（Ｎ，ｐ，ｑ）＝（１６７，３，１２８）、（Ｎ，ｐ，ｑ）＝（５０３，３，２５６）の３つの例が挙げられている。

【００６１】

以降、本発明に係る暗号システムの実施の形態では、システムパラメータＮをＮ＝１６７とした場合の説明を行う。

【００６２】

（２）ＮＴＲＵ暗号方式の多項式演算

ＮＴＲＵ暗号方式は、多項式の演算により暗号化と復号化を行う公開鍵暗号方式である。まず、ＮＴＲＵ暗号方式で扱う多項式は、上記システムパラメータＮに対し、Ｎ－１次元以下の多項式であり、例えばＮ＝５のとき、Ｘ＾４＋Ｘ＾３＋１等の多項式である。ここで、「Ｘ＾ａ」はＸのａ乗を意味することとする。また、暗号化時あるいは復号化時に用いる、公開鍵ｈ、秘密鍵ｆ、平文ｍ、乱数ｒ、暗号文ｃはいずれも、Ｎ－１次元以下の多項式として表現される（以降、それぞれを公開鍵多項式ｈ、秘密鍵多項式ｆ、平文多項式ｍ、乱数多項式ｒ、暗号文多項式ｃと呼ぶ）。

【００６３】

そして、多項式演算は、上記システムパラメータＮに対し、Ｘ＾Ｎ＝１という関係式を用いて、演算結果が常にＮ－１次元以下の多項式になるように演算される。例えば、Ｎ＝５の場合、多項式Ｘ＾４＋Ｘ＾２＋１と多項式Ｘ＾３＋Ｘの積は、多項式と多項式の積を×、整数と多項式の積を・とすると、Ｘ＾５＝１という関係から、

（Ｘ＾４＋Ｘ＾２＋１）×（Ｘ＾３＋Ｘ）

＝Ｘ＾７＋２・Ｘ＾５＋２・Ｘ＾３＋Ｘ

＝Ｘ＾２×１＋２・１＋２・Ｘ＾３＋Ｘ

＝２・Ｘ＾３＋Ｘ＾２＋Ｘ＋２

というように、常にＮ－１次元以下の多項式になるように演算される。

【００６４】

（３）ＮＴＲＵ暗号方式の暗号化

暗号化時には、以下に述べる乱数多項式ｒと公開鍵多項式ｈとを用いて、平文多項式ｍに多項式演算である暗号化アルゴリズムＥを施して、暗号文多項式ｃ＝Ｅ（ｍ，ｒ，ｈ）を生成する。ここで、Ｅ（ｍ，ｒ，ｈ）は、ＮＴＲＵ暗号方式の暗号化アルゴリズムＥに、平文多項式ｍ、乱数多項式ｒ及び公開鍵多項式ｈを入力して得られる多項式演算の結果である。暗号化アルゴリズムＥについては非特許文献２に詳しく述べられており、ここでは説明を省略する。

【００６５】

なお、ＮＴＲＵ暗号方式では、乱数多項式ｒを生成するためのパラメータｄが予め決められており、乱数多項式ｒは、ｄ個の係数が１であり、かつｄ個の係数が－１であり、かつ他の係数は０となるように選ぶ。すなわち、乱数多項式ｒはＮ－１次元以下の多項式であり、０次元（定数項）からＮ－１次元まで、Ｎ個の係数があるが、このＮ個の係数のうち、ｄ個の係数が１であり、かつｄ個の係数が－１であり、かつ（Ｎ－２ｄ）個の係数は０となるように選ぶ。非特許文献２によれば、パラメータＮがＮ＝１６７の場合、ｄ＝１８である。すなわち、１８個の係数が１であり、かつ１８個の係数が－１であり、１３１（＝１６７－３６）個の係数が０となるように乱数多項式ｒを選ぶ。

【００６６】

（４）ＮＴＲＵ暗号方式の復号化

復号化時には、秘密鍵多項式ｆを用いて、暗号文多項式ｃに多項式演算である復号アルゴリズムＤを施して、復号文多項式ｍ’＝Ｄ（ｃ，ｆ）を生成する。ここで、Ｄ（ｃ，ｆ）は、ＮＴＲＵ暗号方式の復号アルゴリズムＤに、暗号文多項式ｃ、及び秘密鍵多項式ｆを入力して得られる多項式演算の結果である。復号アルゴリズムＤについては非特許文献２に詳しく述べられており、ここでは説明を省略する。

【００６７】

（５）ＮＴＲＵ暗号方式の復号エラー

ところで、このＮＴＲＵ暗号方式は、復号文多項式ｍ’が平文多項式ｍと異なる場合が発生する。この場合は、復号時に正しく平文多項式ｍが得られないこと

になる。このことを復号エラーが発生するという。

【００６８】

（実施の形態１）

＜暗号システム１の構成＞

本発明の実施の形態１における暗号システム１の全体構成を図１に示す。この暗号システム１は、ＮＴＲＵ暗号を用いて鍵カプセル化メカニズムによる鍵配送を行って暗号化通信を行う暗号システムであり、暗号装置１１０と、復号装置１２０とから構成され、暗号装置１１０と復号装置１２０とは、通信路１３０を介して接続されている。

【００６９】

＜暗号装置１１０の構成＞

図２は、実施の形態１における暗号装置１１０の構成図である。

【００７０】

暗号装置１１０は、図２に示すように、公開鍵入力部１１１、乱数生成部１１２、第１関数部１１３、暗号化部１１４、送信部１１７、共通鍵暗号部１１８及び共通鍵暗号文送信部１１９から構成される。

【００７１】

（１）公開鍵入力部１１１

公開鍵入力部１１１は、外部から復号装置１２０の公開鍵多項式ｈを受け取り、公開鍵多項式ｈを暗号化部１１４へ出力する。

【００７２】

（２）乱数生成部１１２

乱数生成部１１２は、乱数ｓを生成して、乱数ｓを第１関数部１１３と暗号化部１１４へ出力する。

【００７３】

（３）第１関数部１１３

第１関数部１１３は、乱数生成部１１２から乱数ｓを受け取り、乱数ｓの関数値Ｇ（ｓ）を生成する。そして、関数値Ｇ（ｓ）から共有鍵Ｋと乱数値ｕを生成して、乱数値ｕを暗号化部１１４へ出力し、共有鍵Ｋを共通鍵暗号部１１８へ出

力する。

【００７４】

ここでは、関数Ｇは出力長が２ｋビットのハッシュ関数とし、Ｇ（ｓ）の上位ｋビットを乱数値ｕとし、Ｇ（ｓ）の下位ｋビットを共有鍵Ｋとする。

【００７５】

（４）暗号化部１１４

暗号化部１１４は、公開鍵入力部１１１から公開鍵多項式ｈを受け取り、乱数生成部１１２から乱数ｓを受け取り、第１関数部１１３から乱数値ｕを受け取る。そして、公開鍵多項式ｈと乱数値ｕを用いて乱数ｓの第１暗号文ｃ１を生成し、第１暗号文ｃ１を送信部１１７へ出力する。

【００７６】

ここでは、第１暗号文ｃ１はＮＴＲＵ暗号による暗号文とし、以下のように生成する。

【００７７】

まず、ＮＴＲＵ暗号のパラメータｄに対し、ｄ個の係数が１であり、かつｄ個の係数が－１であり、かつその他の係数が０となる乱数多項式ｒを乱数値ｕから一意に求まるように生成する。これは、例えば、乱数値ｕを擬似乱数系列の初期値（乱数シード）として設定し、｛０，１，．．．，Ｎ－１｝から重複しない擬似乱数２ｄ個を生成し、最初のｄ個を擬似乱数の次元の係数を１、残りのｄ個の擬似乱数の次元の係数を－１とし、他の次元の係数は０とすることで生成できる。そして、乱数ｓをＮＴＲＵ暗号の暗号アルゴリズムＥに適用できるように、乱数ｓの下位ｂビット目の値をＸ＾ｂの係数として乱数多項式ｓｐを構成して、乱数多項式ｓｐに変換する。すなわち、ｓ＝１００１０（ビット表現）の場合、ｓｐ＝Ｘ＾５＋Ｘ＾２と変換する。そして、公開鍵多項式ｈを使用して、乱数多項式ｒを用いて乱数多項式ｓｐに前記暗号アルゴリズムＥを施して、暗号文多項式Ｅ（ｓｐ，ｒ，ｈ）を生成し、第１暗号文ｃ１をｃ１＝Ｅ（ｓｐ，ｒ，ｈ）とする。

【００７８】

（５）送信部１１７

送信部１１７は、暗号化部１１４から第１暗号文ｃ１を受け取り、第１暗号文ｃ１を通信路１３０を介して復号装置１２０へ送信する。

【００７９】

（６）共通鍵暗号部１１８

共通鍵暗号部１１８は、例えばＤＥＳ暗号方式のような共通鍵暗号アルゴリズムＳｙｍを有している。

【００８０】

共通鍵暗号では、暗号鍵Ｋを用いて、平文ｍに共通鍵暗号アルゴリズムＳｙｍを施して、暗号文ｃ＝Ｓｙｍ（ｍ，Ｋ）を生成し、暗号鍵Ｋを用いて、暗号文ｃに共通鍵暗号アルゴリズムＳｙｍを施して、復号文ｍ’＝Ｓｙｍ（ｃ，Ｋ）を生成する。ここで、暗号文生成時に用いた暗号鍵Ｋと復号文生成時に用いる暗号鍵Ｋが同一であれば、ｍ’＝ｍとなる。なお、共通鍵暗号及びＤＥＳ暗号方式については、非特許文献１に詳しく述べられているため、ここでの詳細な説明は省略する。

【００８１】

共通鍵暗号部１１８は、外部から複数の平文ｍｉ（１≦ｉ≦ｎ）を受け取り、第１関数部１１３から共有鍵Ｋを受け取り、共有鍵Ｋを使用して平文ｍｉ（１≦ｉ≦ｎ）に共通鍵暗号アルゴリズムＳｙｍを施して、共通鍵暗号文Ｃｉ＝Ｓｙｍ（ｍｉ，Ｋ）（１≦ｉ≦ｎ）を生成する。

【００８２】

そして、共通鍵暗号部１１８は、共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を共通鍵暗号文送信部１１９へ出力する。

【００８３】

（７）共通鍵暗号文送信部１１９

共通鍵暗号文送信部１１９は、共通鍵暗号化部１１８から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受け取り、通信路１３０を介して復号装置１２０へ送信する。

【００８４】

＜暗号装置１１０の動作＞

ここで、以上に述べた暗号装置１１０の動作について、図３に示すフローチャ

ートを用いて説明する。

【００８５】

まず、公開鍵入力部１１１は、外部から復号装置１２０の公開鍵多項式ｈを受け取り、公開鍵多項式ｈを暗号化部１１４へ出力する（ステップＳ１０１）。

【００８６】

次に、乱数生成部１１２は、乱数ｓを生成して、乱数ｓを第１関数部１１３と暗号化部１１４へ出力する（ステップＳ１０２）。

【００８７】

次に、第１関数部１１３は、乱数生成部１１２から乱数ｓを受け取り、乱数ｓの関数値Ｇ（ｓ）を生成する（ステップＳ１０３）。そして、第１関数部１１３は、関数値Ｇ（ｓ）から乱数値ｕと共有鍵Ｋを生成して、乱数値ｕを暗号化部１１４へ出力し、共有鍵Ｋを共通鍵暗号部１１８へ出力する（ステップＳ１０４）。

【００８８】

次に、暗号化部１１４は、公開鍵入力部１１１から公開鍵多項式ｈを受け取り、乱数生成部１１２から乱数ｓを受け取り、第１関数部１１３から乱数値ｕを受け取る。そして、暗号化部１１４は、公開鍵多項式ｈと乱数値ｕを用いて乱数ｓの第１暗号文ｃ１を生成し、第１暗号文ｃ１を送信部１１７へ出力する（ステップＳ１０５）。

【００８９】

次に、送信部１１７は、暗号化部１１４から第１暗号文ｃ１を受け取り、第１暗号文ｃ１を通信路１３０を介して復号装置１２０へ送信する（ステップＳ１０６）。

【００９０】

次に、共通鍵暗号部１１８は、外部から複数の平文ｍｉ（１≦ｉ≦ｎ）を受け取り、第１関数部１１３から共有鍵Ｋを受け取り、共有鍵Ｋを使用して平文ｍｉ（１≦ｉ≦ｎ）に共通鍵暗号アルゴリズムＳｙｍを施して、共通鍵暗号文Ｃｉ＝Ｓｙｍ（ｍｉ，Ｋ）（１≦ｉ≦ｎ）を生成し、共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を共通鍵暗号文送信部１１９へ出力する（ステップＳ１０７）。

【００９１】

次に、共通鍵暗号文送信部１１９は、共通鍵暗号化部１１８から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受け取り、通信路１３０を介して復号装置１２０へ送信して処理を終了する（ステップＳ１０８）。

【００９２】

＜復号装置１２０の構成＞

図４は、実施の形態１における復号装置１２０の構成図である。

【００９３】

復号装置１２０は、図４に示すように、秘密鍵入力部１２１、受信部１２２、復号化部１２３、第２関数部１２６、比較部１２７、共通鍵復号部１２８及び共通鍵暗号文受信部１２９から構成される。

【００９４】

（１）秘密鍵入力部１２１

秘密鍵入力部１２１は、外部から復号装置１２０の秘密鍵多項式ｆと公開鍵多項式ｈを受け取り、秘密鍵多項式ｆを復号化部１２３へ出力し、公開鍵多項式ｈを比較部１２７へ出力する。

【００９５】

（２）受信部１２２

受信部１２２は、通信路１３０を介して暗号装置１１０から第１暗号文ｃ１を受け取り、第１暗号文ｃ１を復号化部１２３へ出力する。

【００９６】

（３）復号化部１２３

復号化部１２３は、秘密鍵入力部１２１から秘密鍵多項式ｆを受け取り、受信部１２２から第１暗号文ｃ１を受け取る。そして、秘密鍵多項式ｆを用いて、第１暗号文ｃ１を復号して復号乱数ｓ’を生成し、第１暗号文ｃ１と復号乱数ｓ’を比較部１２７へ出力し、復号乱数ｓ’を第２関数部１２６へと出力する。

【００９７】

ここでは、復号乱数ｓ’はＮＴＲＵ暗号による復号文とし、以下のように生成する。

【００９８】

まず、秘密鍵多項式ｆを使用して、第１暗号文ｃ１に前記復号アルゴリズムＤを施して、復号乱数多項式ｓｐ’＝Ｄ（ｃ１，ｆ）を生成する。そして、復号乱数多項式ｓｐ’は、ＮＴＲＵ暗号の復号文であり多項式で表現されているので、復号乱数多項式ｓｐ’のｂ次元の項Ｘ＾ｂの係数を下位ｂビット目の値として復号乱数ｓ’を構成して、復号乱数ｓ’に変換する。すなわち、ｓｐ’＝Ｘ＾５＋Ｘ＾２の場合、ｓ’＝１００１０（ビット表現）と変換する。

【００９９】

（４）第２関数部１２６

第２関数部１２６は、第１関数部１１３と同じ関数Ｇのアルゴリズムを有している。

【０１００】

第２関数部１２６は、復号化部１２３から復号乱数ｓ’を受け取り、復号乱数ｓ’の関数値Ｇ（ｓ’）を生成する。そして、関数値Ｇ（ｓ’）から乱数値ｕ’と共有鍵Ｋ’を生成して、乱数値ｕ’と共有鍵Ｋ’を比較部１２７へ出力する。

【０１０１】

（５）比較部１２７

比較部１２７は、秘密鍵入力部１２１から公開鍵多項式ｈを受け取り、復号化部１２３から第１暗号文ｃ１と復号乱数ｓ’を受け取り、第２関数部１２６から乱数値ｕ’と共有鍵Ｋ’を受け取る。そして、公開鍵多項式ｈと乱数値ｕ’を用いて、暗号化部１１４と同様にして復号乱数ｓ’を暗号化して第１再暗号文ｃ１’を生成する。そして、ｃ１’＝ｃ１であれば、共有鍵Ｋ’を共通鍵復号部１２８へ出力する。

【０１０２】

（６）共通鍵復号部１２８

共通鍵復号部１２８は、共通鍵暗号部１１８が有する共通鍵暗号アルゴリズムＳｙｍを予め有している。

【０１０３】

共通鍵復号部１２８は、比較部１２７から共有鍵Ｋ’を受け取り、共通鍵暗号

文受信部１２９から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受け取り、共有鍵Ｋ’を使用して共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）に共通鍵暗号アルゴリズムＳｙｍを施して、復号文ｍｉ’＝Ｓｙｍ（Ｃｉ，Ｋ）（１≦ｉ≦ｎ）を生成する。

【０１０４】

そして、共通鍵復号部１２８は、復号文ｍｉ’（１≦ｉ≦ｎ）を外部へ出力する。

【０１０５】

（７）共通鍵暗号文受信部１２９

共通鍵暗号文受信部１２９は、通信路１３０を介して暗号装置１１０から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受信し、共通鍵復号部１２８へ出力する。

【０１０６】

＜復号装置１２０の動作＞

ここで、以上に述べた復号装置１２０の動作について、図５に示すフローチャートを用いて説明する。

【０１０７】

まず、秘密鍵入力部１２１は、外部から復号装置１２０の秘密鍵多項式ｆと公開鍵多項式ｈを受け取り、秘密鍵多項式ｆを復号化部１２３へ出力し、公開鍵多項式ｈを比較部１２７へ出力する（ステップＳ１５１）。

【０１０８】

次に、受信部１２２は、通信路１３０を介して暗号装置１１０から第１暗号文多項式ｃ１を受け取り、第１暗号文多項式ｃ１を復号化部１２３へ出力する（ステップＳ１５２）。

【０１０９】

次に、復号化部１２３は、秘密鍵入力部１２１から秘密鍵多項式ｆを受け取り、受信部１２２から第１暗号文ｃ１を受け取る。そして、復号化部１２３は、秘密鍵多項式ｆを用いて、第１暗号文ｃ１を復号して復号乱数ｓ’を生成し、第１暗号文ｃ１と復号乱数ｓ’を比較部１２７へ出力し、復号乱数ｓ’を第２関数部１２６へ出力する（ステップＳ１５３）。

【０１１０】

次に、第２関数部１２６は、復号化部１２３から復号乱数ｓ’を受け取り、復号乱数ｓ’の関数値Ｇ（ｓ’）を生成する（ステップＳ１５４）。そして、関数値Ｇ（ｓ’）から乱数値ｕ’と共有鍵Ｋ’を生成して、乱数値ｕ’と共有鍵Ｋ’を比較部１２７へ出力する（ステップＳ１５５）。

【０１１１】

次に、比較部１２７は、復号化部１２３から第１暗号文ｃ１を受け取り、第２関数部１２６から乱数値ｕ’と共有鍵Ｋ’を受け取る（ステップＳ１５６）。そして、第一暗号文ｃ１が乱数値ｕ’を用いた復号乱数ｓ’の暗号文であるかどうかチェックを行い、第１暗号文ｃ１が復号乱数ｓ’の暗号文であれば、ステップＳ１６２へ処理を移し、等しくなければ処理を終了する（ステップＳ１５７）。そして、比較部１２７は、共有鍵Ｋ’を共通鍵復号部１２８へ出力する（ステップＳ１５８）。

【０１１２】

次に、共通鍵暗号文受信部１２９は、通信路１３０を介して暗号装置１１０から暗号文Ｃｉ（１≦ｉ≦ｎ）を受信し、共通鍵復号部１２８へ出力する（ステップＳ１５９）。

【０１１３】

次に、共通鍵復号部１２８は、比較部１２７から共有鍵Ｋ’を受け取り、共通鍵暗号文受信部１２９から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受け取り、共有鍵Ｋ’を使用して共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）に共通鍵暗号アルゴリズムＳｙｍを施して、復号文ｍｉ’＝Ｓｙｍ（Ｃｉ，Ｋ）（１≦ｉ≦ｎ）を生成し、復号文ｍｉ’（１≦ｉ≦ｎ）を外部へ出力して処理を終了する（ステップＳ１６０）。

【０１１４】

＜暗号システム１の動作検証＞

以下に、実施の形態１における暗号システム１の全体の動作について説明する。

【０１１５】

まず、暗号装置１１０は、復号装置１２０の公開鍵多項式ｈを入力とし、乱数

ｓを生成して、関数値Ｇ（ｓ）から乱数値ｕと共有鍵Ｋを導出する。そして、暗号装置１１０は、乱数ｓを、公開鍵多項式ｈと乱数値ｕを用いてＮＴＲＵ暗号で暗号化して第１暗号文ｃ１を生成し、第１暗号文ｃ１を通信路１３０を介して復号装置１２０へ送信する。

【０１１６】

すなわち、この暗号装置１１０は、以下の処理を行い、第１暗号文ｃ１を復号装置１２０へ送信する。

【０１１７】

・乱数ｓを生成する。

【０１１８】

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からｕ、Ｋを生成する。

【０１１９】

・公開鍵多項式ｈと乱数値ｕを用いて乱数ｓの第１暗号文ｃ１を生成する。

【０１２０】

・共有鍵Ｋと第１暗号文ｃ１を出力する。

【０１２１】

次に、暗号装置１１０は、導出した共有鍵Ｋを用いて、外部から入力された平文ｍｉ（１≦ｉ≦ｎ）を共通鍵暗号で暗号化して暗号文Ｃｉ（１≦ｉ≦ｎ）を生成し、通信路１３０を介して復号装置１２０へ送信する。

【０１２２】

一方、復号装置１２０は、復号装置１２０の秘密鍵多項式ｆ及び公開鍵多項式ｈを入力とし、通信路１３０を介して暗号装置１１０から第１暗号文ｃ１を受信し、第１暗号文ｃ１を秘密鍵多項式ｆを用いて復号して復号乱数ｓ’を生成する。そして、復号乱数ｓ’の関数値Ｇ（ｓ’）から乱数値ｕ’と共有鍵Ｋ’を導出する。そして、復号乱数ｓ’を暗号化して第１再暗号文ｃ１’を生成し、ｃ１’＝ｃ１であれば、共有鍵Ｋ’を出力する。

【０１２３】

すなわち、この復号装置１２０は、以下の処理を行い、共有鍵Ｋ’を導出する。

【０１２４】

・秘密鍵多項式ｆを用いて第１暗号文ｃ１を復号してｓ’を生成する。

【０１２５】

・Ｇ（ｓ’）を生成し、Ｇ（ｓ’）からｕ’、Ｋ’を生成する。

【０１２６】

・公開鍵多項式ｈ、乱数値ｕ’を用いてｓ’の第１再暗号文ｃ１’を生成する。

【０１２７】

・ｃ１’＝ｃ１が成立するかどうかチェックする。成立すれば共有鍵Ｋ’を出力する。

【０１２８】

ここで、暗号装置１１０で用いられた公開鍵多項式ｈに対応する正しい秘密鍵多項式ｆが復号装置１２０で用いられれば、第１暗号文ｃ１は正しく復号されて、復号乱数ｓ’はｓ’＝ｓとなり、従って、Ｇ（ｓ’）から導出される乱数値ｕ’はｕ’＝ｕとなり、共有鍵Ｋ’はＫ’＝Ｋとなる。そして、ｓ’＝ｓ及びｕ’＝ｕが成り立つので、ｃ１’＝ｃ１が成り立ち、復号装置１２０は暗号装置１１０ｂと同じ共有鍵Ｋを導出できることになる。

【０１２９】

次に、復号装置１２０は、導出した共有鍵Ｋ’（＝Ｋ）を用いて、通信路を介して暗号装置１１０から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を共通鍵暗号で復号して復号文ｍｉ’（１≦ｉ≦ｎ）を生成して外部へ出力する。今、共通鍵暗号文生成時に用いた暗号鍵Ｋと復号文生成時に用いる暗号鍵Ｋ’は同一なので、復号装置１２０は、正しくｍｉ’＝ｍｉ（１≦ｉ≦ｎ）を得ることができる。

【０１３０】

なお、復号エラーが発生した場合には、復号乱数ｓ’と乱数ｓとは異なるので、Ｇ（ｓ’）から導出される乱数値ｕ’及び共有鍵Ｋ’はそれぞれｕ、Ｋとは異なる。しかし、この場合、ｓ’、ｕ’がそれぞれｓ、ｕと異なるために第１再暗号文ｃ１’が第１暗号文ｃ１と異なるので、復号装置１２０は、共有鍵Ｋ’を出力しない。

【０１３１】

＜実施の形態１における効果＞

ＲＳＡ－ＫＥＭアルゴリズムは、暗号文Ｃから秘密鍵を知らなければ導出できないランダムな要素ｓをハッシュ関数Ｇに入力して共有鍵Ｋを導出するようにしていた。しかしながら、ＮＴＲＵ暗号は、鍵カプセル化メカニズムであるＲＳＡ－ＫＥＭアルゴリズムを適用して共有鍵の配送を行おうとすると、復号エラーが発生する場合があるため、秘密鍵を用いてもランダムな要素ｓが導出できず、従って正しくない共有鍵Ｋ’を導出する場合があった。

【０１３２】

しかしながら、この暗号システム、暗号装置及び復号装置は、乱数ｓのハッシュ関数値Ｇ（ｓ）から共有鍵に加えて乱数値ｕを生成し、復号装置が乱数値ｕと公開鍵多項式ｈを用いて復号乱数ｓ’を再暗号化して第１再暗号文ｃ１’を生成し、第１再暗号文ｃ１’が第１暗号文ｃ１と同じ値でない限り共有鍵Ｋ’を出力しないようにしたので、復号エラーが発生した場合、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できるようになった。

【０１３３】

＜変形例＞

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

【０１３４】

（１）用いるＮＴＲＵ暗号のパラメータはＮ＝１６７に限定されず、他のパラメータでもよい。

【０１３５】

（２）暗号化部１１４、復号化部１２３で行われるビット列と多項式との変換方法は、この方法に限られず他の変換方法でもよい。

【０１３６】

例えば、ビット列と多項式を１対１に対応させる関数もしくは関数値のテーブルを用いて変換してもよい。

【０１３７】

（３）暗号化部１１４、復号化部１２３で用いる公開鍵暗号は、暗号化部１１４において、乱数ｓを公開鍵と乱数値ｕを用いて暗号化して第１暗号文ｃ１を生成し、復号化部１２３において、第１暗号文ｃ１を秘密鍵で復号して乱数値ｓと等しい復号乱数ｓ’を生成できればよい。従って、暗号化部１１４、復号化部１２３で用いる公開鍵暗号は、ＮＴＲＵ暗号以外に、どんな公開鍵暗号でも利用できる。

【０１３８】

例えば、ＥｌＧａｍａｌ暗号ならば、ｈ、ｆをそれぞれＥｌＧａｍａｌ暗号の公開鍵、秘密鍵とし、暗号化部１１４において、乱数ｓをｈとｕを用いて暗号化してｃ１を生成し、復号化部１２３において、ｃ１をｆを用いて復号してｓ’を生成すればよい。

【０１３９】

なお、ＥｌＧａｍａｌ暗号について非特許文献１に詳細に記載されているため、ここでは説明を省略する。

【０１４０】

（４）第１関数部１１３は、関数値Ｇ（ｓ）の上位ｋビットを乱数値ｕとして下位ｋビットを共有鍵Ｋとする以外に、関数値Ｇ（ｓ）から乱数値ｕと共有鍵Ｋを導出すれば他の方法でもよい。

【０１４１】

（５）乱数値ｕは、第１関数部１１３及び第２関数部１２６で生成される以外にも、暗号装置１１０と復号装置１２０とで同じ値を得られれば、他の生成方法でもよい。

【０１４２】

例えば、任意の関数Ｆｕｎｃに対し、ｕ＝Ｆｕｎｃ（ｓ）として暗号装置１１０と復号装置１２０とで同じ値を得られるようにしてもよい。すなわち、

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からＫを生成する。

【０１４３】

・Ｆｕｎｃ（ｓ）を生成し、ｕ＝Ｆｕｎｃ（ｓ）とする。

としてもよい。

【０１４４】

（６）さらに、乱数値ｕは、第１関数部１１３及び第２関数部１２６で生成される以外にも、暗号装置１１０と復号装置１２０とで同じ値を得られればよいため、暗号装置１１０が乱数値ｕを復号装置１２０ｂに直接送信してもよい。

【０１４５】

すなわち、以下のように、第１暗号文ｃ１と乱数値ｕを復号装置１２０に送信してもよい。また、乱数値ｕは暗号化して送信されてもよい。

【０１４６】

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からＫを生成する。

【０１４７】

・乱数値ｕは、別途、暗号装置１１０ｂから１２０ｂへ送信される。

【０１４８】

（７）さらに、乱数値ｕは、暗号装置１１０と復号装置１２０とで同じ値を得られればよいため、乱数値ｕの部分情報を第１関数部１１３及び第２関数部１２６で生成し、乱数値ｕの残りの部分情報を暗号装置１１０から復号装置１２０に直接送信してもよい。

【０１４９】

例えば、以下のように、第１暗号文ｃ１と乱数値ｕ２を復号装置１２０に送信してもよい。また、乱数値ｕ２は暗号化して送信されてもよい。

【０１５０】

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からＫ、ｕ１を生成する。

【０１５１】

・乱数値ｕ２は、別途、暗号装置１１０から１２０へ送信される。

【０１５２】

・乱数値ｕは、ｕ＝ｕ１　ｘｏｒ　ｕ２から生成される。

【０１５３】

（８）なお、復号エラー発生により暗号装置１１０と復号装置１２０との間で異なる鍵が導出されるのを防止するため、第１再暗号文ｃ１’が第１暗号文ｃ１

と同じ値かどうかを検証して共有鍵Ｋ’を出力する代わりに、暗号装置１１０が乱数ｓ、乱数値ｕ、共有鍵Ｋのいずれかのハッシュ関数値を生成し、復号装置１２０がこのハッシュ関数値を検証して共有鍵Ｋ’を出力するか否かを決定してもよい。

【０１５４】

例えば、暗号装置１１０が乱数ｓのハッシュ関数値を生成し、復号装置１２０がこのハッシュ関数値を検証する場合、暗号装置１１０は、図６に示すように、

・第１関数部１１３が、Ｇ（ｓ）を生成し、Ｇ（ｓ）からＫを生成する。

【０１５５】

・暗号化部１１４が、公開鍵多項式ｈを用いて乱数ｓの第１暗号文ｃ１と、ハッシュ関数値Ｈ（ｓ）を生成する。

【０１５６】

・送信部１１７が、第１暗号文ｃ１とハッシュ関数値Ｈ（ｓ）を送信する。

という処理を行い、復号装置１２０は、図７に示すように、

・受信部１２２が、第１暗号文ｃ１とハッシュ関数値Ｈ（ｓ）を受信する。

【０１５７】

・復号化部１２３が、秘密鍵多項式ｆを用いて第１暗号文ｃ１を復号してｓ’を生成する。

【０１５８】

・第２関数部１２６が、Ｇ（ｓ’）を生成し、Ｇ（ｓ’）からＫ’を生成する。

【０１５９】

・比較部１２７がＨ（ｓ’）を生成し、Ｈ（ｓ’）＝Ｈ（ｓ）が成立するかどうかチェックする。成立すれば共有鍵Ｋ’を出力する。

という処理を行ってもよい。

【０１６０】

さらに、この場合、安全性を高めるために、特許文献１に開示されている方法を用いて、乱数ｓに付加情報を附したものを暗号化して第１暗号文ｃ１を生成してもよい。すなわち、図６において、暗号化部１１４が付加情報Ｒａを生成し、

ｓとＲａのビット結合ｓ｜｜Ｒａの値を暗号化して第１暗号文ｃ１を生成し、図７において、復号化部１２３が、第１暗号文ｃ１を復号してｓ’｜｜Ｒａ’を生成し、Ｒａ’を除去して復号乱数ｓ’を生成してもよい。なお、特許文献１に開示されている通り、ｓ｜｜Ｒａの値の代わりに、ｓとＲａの可逆変換Ｆ（ｓ，Ｒａ）の値を用いてもよい。

【０１６１】

（９）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【０１６２】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、半導体メモリ、ハードディスクドライブ、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ等、に記録したものとしてもよい。

【０１６３】

（１０）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０１６４】

（実施の形態２）

本発明の実施の形態２における暗号システム２は、暗号システム１を基本にして変形した暗号システムであり、関数値Ｇ（ｓ）から乱数値ｕと共有鍵Ｋの他にさらに検証値ａを生成する点と、暗号装置が、乱数ｓを暗号化した第１暗号文ｃ１を生成して送信する代わりに、検証値ａを暗号化した第１暗号文ｃ１と、乱数ｓを検証値ａに基づいて暗号化して第２暗号文ｃ２とを生成して送信する点が暗号システム１と異なる。

【０１６５】

以下、暗号システム２について、上記差異点を中心に詳しく説明する。

【０１６６】

＜暗号システム２の構成＞

本発明の実施の形態２における暗号システム２の全体構成を図８に示す。この暗号システム２は、ＮＴＲＵ暗号を用いて鍵配送を行う暗号システムであり、暗号装置１１０ｂと、復号装置１２０ｂとから構成され、暗号装置１１０ｂと復号装置１２０ｂとは、通信路１３０を介して接続されている。

【０１６７】

＜暗号装置１１０ｂの構成＞

図９は、実施の形態２における暗号装置１１０ｂの構成図である。

【０１６８】

暗号装置１１０ｂは、図９に示すように、公開鍵入力部１１１、乱数生成部１１２ｂ、第１関数部１１３ｂ、暗号化部１１４ｂ、乱数マスク部１１６、送信部１１７ｂ、共通鍵暗号部１１８及び共通鍵暗号文送信部１１９から構成される。

【０１６９】

以下、暗号システム１と異なる乱数生成部１１２ｂ、第１関数部１１３ｂ、暗号化部１１４ｂ、乱数マスク部１１６及び送信部１１７ｂについてその構成と動作を説明する。

【０１７０】

（１）乱数生成部１１２ｂ

乱数生成部１１２ｂは、乱数ｓを生成して、乱数ｓを第１関数部１１３ｂと乱数マスク部１１６へ出力する。

【０１７１】

（２）第１関数部１１３ｂ

第１関数部１１３ｂは、乱数生成部１１２ｂから乱数ｓを受け取り、乱数ｓの関数値Ｇ（ｓ）を生成する。そして、関数値Ｇ（ｓ）から検証値ａと共有鍵Ｋと乱数値ｕを生成して、検証値ａと乱数値ｕを暗号化部１１４ｂへ出力し、共有鍵Ｋを共通鍵暗号部１１８へ出力し、検証値ａを乱数マスク部１１６へ出力する。

【０１７２】

ここでは、関数Ｇは出力長が３ｋビットのハッシュ関数とし、Ｇ（ｓ）の上位ｋビットを検証値ａとし、Ｇ（ｓ）の中間のｋビットを共有鍵Ｋし、Ｇ（ｓ）の下位ｋビットを乱数値ｕとする。

【０１７３】

（３）暗号化部１１４ｂ

暗号化部１１４ｂは、公開鍵入力部１１１から公開鍵多項式ｈを受け取り、第１関数部１１３ｂから検証値ａと乱数値ｕを受け取る。そして、公開鍵多項式ｈと乱数値ｕを用いて検証値ａの第１暗号文ｃ１を生成し、第１暗号文ｃ１を送信部１１７ｂへ出力する。

【０１７４】

ここでは、第１暗号文ｃ１はＮＴＲＵ暗号による暗号文とし、以下のように生成する。

【０１７５】

まず、ＮＴＲＵ暗号のパラメータｄに対し、ｄ個の係数が１であり、かつｄ個の係数が－１であり、かつその他の係数が０となる乱数多項式ｒを乱数値ｕから一意に求まるように生成する。これは、例えば、乱数値ｕを擬似乱数系列の初期値（乱数シード）として設定し、｛０，１，．．．，Ｎ－１｝から重複しない擬似乱数２ｄ個を生成し、最初のｄ個を擬似乱数の次元の係数を１、残りのｄ個の擬似乱数の次元の係数を－１とし、他の次元の係数は０とすることで生成できる。そして、検証値ａをＮＴＲＵ暗号の暗号アルゴリズムＥに適用できるように、検証値ａの下位ｂビット目の値をＸ＾ｂの係数として検証値多項式ａｐを構成して、検証値多項式ａｐに変換する。すなわち、ａ＝１００１０（ビット表現）の場合、ａｐ＝Ｘ＾５＋Ｘ＾２と変換する。そして、公開鍵多項式ｈを使用して、乱数多項式ｒを用いて検証値多項式ａｐに前記暗号アルゴリズムＥを施して、暗号文多項式Ｅ（ａｐ，ｒ，ｈ）を生成し、第１暗号文ｃ１をｃ１＝Ｅ（ａｐ，ｒ，ｈ）とする。

【０１７６】

（４）乱数マスク部１１６

乱数マスク部１１６は、乱数生成部１１２ｂから乱数ｓを受け取り、第１関数部１１３ｂから検証値ａを受け取る。そして、第２暗号文ｃ２としてｃ２＝ｓｘｏｒ　ａを生成し、第２暗号文ｃ２を送信部１１７ｂへ出力する。ここで、ｘｏｒは排他的論理和演算を表す。

【０１７７】

（５）送信部１１７ｂ

送信部１１７ｂは、暗号化部１１４ｂから第１暗号文ｃ１を受け取り、乱数マスク部１１６から第２暗号文ｃ２を受け取り、第１暗号文ｃ１と第２暗号文ｃ２を通信路１３０を介して復号装置１２０ｂへ送信する。

【０１７８】

＜復号装置１２０ｂの構成＞

図１０は、実施の形態２における復号装置１２０ｂの構成図である。

【０１７９】

復号装置１２０ｂは、図１０に示すように、秘密鍵入力部１２１、受信部１２２ｂ、復号化部１２３ｂ、乱数マスク除去部１２５、第２関数部１２６ｂ、比較部１２７ｂ、共通鍵復号部１２８及び共通鍵暗号文受信部１２９から構成される。

【０１８０】

以下、暗号システム１と異なる受信部１２２ｂ、復号化部１２３ｂ、乱数マスク除去部１２５、第２関数部１２６ｂ及び比較部１２７ｂについてその構成と動作を説明する。

【０１８１】

（１）受信部１２２ｂ

受信部１２２ｂは、通信路１３０を介して暗号装置１１０ｂから第１暗号文ｃ１と第２暗号文ｃ２を受け取り、第１暗号文ｃ１を復号化部１２３ｂへ出力し、第２暗号文ｃ２を乱数マスク除去部１２５へ出力する。

【０１８２】

（２）復号化部１２３ｂ

復号化部１２３ｂは、秘密鍵入力部１２１から秘密鍵多項式ｆを受け取り、受信部１２２ｂから第１暗号文ｃ１を受け取る。そして、秘密鍵多項式ｆを用いて、第１暗号文ｃ１を復号して復号検証値ａ’を生成し、復号検証値ａ’を乱数マスク除去部１２５へ出力して、第１暗号文ｃ１を比較部１２７ｂに出力する。

【０１８３】

ここでは、復号検証値ａ’はＮＴＲＵ暗号による復号文とし、以下のように生成する。

【０１８４】

まず、秘密鍵多項式ｆを使用して、第１暗号文ｃ１に前記復号アルゴリズムＤを施して、復号検証値多項式ａｐ’＝Ｄ（ｃ１，ｆ）を生成する。そして、復号検証値多項式ａｐ’は、ＮＴＲＵ暗号の復号文であり多項式で表現されているので、復号検証値多項式ａｐ’のｂ次元の項Ｘ＾ｂの係数を下位ｂビット目の値として復号検証値ａ’を構成して、復号検証値ａ’に変換する。すなわち、ａｐ’＝Ｘ＾５＋Ｘ＾２の場合、ａ’＝１００１０（ビット表現）と変換する。

【０１８５】

（３）乱数マスク除去部１２５

乱数マスク除去部１２５は、受信部１２２ｂから第２暗号文ｃ２を受け取り、復号化部１２３ｂから復号検証値ａ’を受け取る。そして、復号乱数ｓ’として、ｓ’＝ｃ２　ｘｏｒ　ａ’を生成し、復号乱数ｓ’を第２関数部１２６ｂへ出力する。

【０１８６】

（４）第２関数部１２６ｂ

第２関数部１２６ｂは、第１関数部１１３ｂと同じ関数Ｇのアルゴリズムを有している。

【０１８７】

第２関数部１２６ｂは、乱数マスク除去部１２５から復号乱数ｓ’を受け取り、復号乱数ｓ’の関数値Ｇ（ｓ’）を生成する。そして、第１関数部１１３ｂと同様にして、関数値Ｇ（ｓ’）から検証値ａ’’と共有鍵Ｋ’と乱数値ｕ’を生成して、検証値ａ’’と共有鍵Ｋ’と乱数値ｕ’を比較部１２７ｂへ出力する。

【０１８８】

（５）比較部１２７ｂ

比較部１２７ｂは、秘密鍵入力部１２１から公開鍵多項式ｈを受け取り、復号化部１２３ｂから第１暗号文ｃ１を受け取り、第２関数部１２６ｂから検証値ａ’’と共有鍵Ｋ’と乱数値ｕ’を受け取る。そして、公開鍵多項式ｈと乱数値ｕ

’を用いて、暗号化部１１４ｂと同様にして検証値ａ’’を暗号化して第１再暗号文ｃ１’を生成する。そして、ｃ１’＝ｃ１であれば、共有鍵Ｋ’を共通鍵暗号部１２８へ出力する。

【０１８９】

＜暗号システム２の動作検証＞

以下に、実施の形態２における暗号システム２の全体の動作について説明する。

【０１９０】

まず、暗号装置１１０ｂは、復号装置１２０ｂの公開鍵多項式ｈを入力とし、乱数ｓを生成して、関数値Ｇ（ｓ）から検証値ａ、共有鍵Ｋ及び乱数値ｕを導出する。そして、暗号装置１１０ｂは、検証値ａを、公開鍵多項式ｈ及び乱数値ｕを用いてＮＴＲＵ暗号で暗号化して第１暗号文ｃ１を生成し、検証値ａに基づき乱数ｓを暗号化して第２暗号文ｃ２＝ｓ　ｘｏｒ　ａを生成する。そして、暗号装置１１０ｂは、第１暗号文ｃ１と第２暗号文ｃ２を通信路１３０を介して復号装置１２０ｂへ送信する。

【０１９１】

すなわち、この暗号装置１１０ｂは、以下の処理を行い、暗号文Ｃ＝（ｃ１，ｃ２）を復号装置１２０ｂへ送信する。

【０１９２】

・乱数ｓを生成する。

【０１９３】

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ、Ｋ、ｕを生成する。

【０１９４】

・公開鍵多項式ｈ、乱数値ｕを用いて検証値ａの第１暗号文ｃ１を生成する。

【０１９５】

・ｃ２＝ｓ　ｘｏｒ　ａを生成する。

【０１９６】

・共有鍵Ｋと暗号文Ｃ＝（ｃ１，ｃ２）を出力する。

【０１９７】

次に、暗号装置１１０ｂは、導出した共有鍵Ｋを用いて、外部から入力された平文ｍｉ（１≦ｉ≦ｎ）を共通鍵暗号で暗号化して暗号文Ｃｉ（１≦ｉ≦ｎ）を生成し、通信路１３０を介して復号装置１２０ｂへ送信する。

【０１９８】

一方、復号装置１２０ｂは、復号装置１２０ｂの秘密鍵多項式ｆ及び公開鍵多項式ｈを入力とし、通信路１３０を介して暗号装置１１０ｂから第１暗号文ｃ１と第２暗号文ｃ２を受信し、第１暗号文ｃ１を秘密鍵多項式ｆを用いて復号して復号検証値ａ’を生成する。そして、復号検証値ａ’に基づき第２暗号文ｃ２を復号して、復号乱数ｓ’＝ｃ２　ｘｏｒ　ａ’を生成する。そして、復号装置１２０ｂは、復号乱数ｓ’の関数値Ｇ（ｓ’）から検証値ａ’’、共有鍵Ｋ’及び乱数値ｕ’を導出する。そして、検証値ａ’’を暗号化して第１再暗号文ｃ１’を生成し、ｃ１’＝ｃ１であれば、共有鍵Ｋ’を出力する。

【０１９９】

すなわち、この復号装置１２０ｂは、以下の処理を行い、共有鍵Ｋ’を導出する。

【０２００】

・秘密鍵多項式ｆを用いて第１暗号文ｃ１を復号してａ’を生成する。

【０２０１】

・ｓ’＝ｃ２　ｘｏｒ　ａ’を生成する。

【０２０２】

・Ｇ（ｓ’）を生成し、Ｇ（ｓ’）からａ’’、Ｋ’、ｕ’を生成する。

【０２０３】

・公開鍵多項式ｈ、乱数値ｕ’を用いてａ’’の第１再暗号文ｃ１’を生成する。

【０２０４】

・ｃ１’＝ｃ１が成立するかどうかチェックする。成立すれば共有鍵Ｋ’を出力する。

【０２０５】

ここで、暗号装置１１０ｂで用いられた公開鍵多項式ｈに対応する正しい秘密

鍵多項式ｆが復号装置１２０ｂで用いられれば、第１暗号文ｃ１は正しく復号されて、復号検証値ａ’はａ’＝ａとなり、第２暗号文ｃ２とａ’から生成される復号乱数ｓ’はｓ’＝ｓとなる。従って、Ｇ（ｓ’）から導出される検証値ａ’’はａ’’＝ａとなり、共有鍵Ｋ’はＫ’＝Ｋとなり、乱数値ｕ’はｕ’＝ｕとなる。そして、ａ’’＝ａ及びｕ’＝ｕが成り立つので、ｃ１’＝ｃ１が成り立ち、復号装置１２０ｂは暗号装置１１０ｂと同じ共有鍵Ｋを導出できることになる。

【０２０６】

次に、復号装置１２０ｂは、導出した共有鍵Ｋ’（＝Ｋ）を用いて、通信路を介して暗号装置１１０ｂから共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を共通鍵暗号で復号して復号文ｍｉ’（１≦ｉ≦ｎ）を生成して外部へ出力する。今、共通鍵暗号文生成時に用いた暗号鍵Ｋと復号文生成時に用いる暗号鍵Ｋ’は同一なので、復号装置１２０ｂは、正しくｍｉ’＝ｍｉ（１≦ｉ≦ｎ）を得ることができる。

なお、復号エラーが発生した場合には、復号検証値ａ’と検証値ａとは異なるので、第２暗号文ｃ２から得られる復号乱数ｓ’はｓと異なる。従って、Ｇ（ｓ’）から導出される乱数値ｕ’及び共有鍵Ｋ’はそれぞれｕ、Ｋとは異なる。しかし、この場合、ａ’、ｕ’がそれぞれｓ、ｕと異なるために第１再暗号文ｃ１’が第１暗号文ｃ１と異なるので、復号装置１２０は、共有鍵Ｋ’を出力しない。

【０２０７】

＜実施の形態２における効果＞

ＲＳＡ－ＫＥＭアルゴリズムは、暗号文Ｃから秘密鍵を知らなければ導出できないランダムな要素ｓをハッシュ関数Ｇに入力して共有鍵Ｋを導出するようにしていた。しかしながら、ＮＴＲＵ暗号は、鍵カプセル化メカニズムであるＲＳＡ－ＫＥＭアルゴリズムを適用して共有鍵の配送を行おうとすると、復号エラーが発生する場合があるため、秘密鍵を用いてもランダムな要素ｓが導出できず、従って正しくない共有鍵Ｋ’を導出する場合があった。

【０２０８】

しかしながら、この暗号システム、暗号装置及び復号装置は、乱数ｓのハッシュ関数値Ｇ（ｓ）から共有鍵に加えて検証値ａと乱数値ｕを生成し、復号装置が乱数値ｕと公開鍵多項式ｈを用いて復号検証値ａ’を再暗号化して第１再暗号文ｃ１’を生成し、第１再暗号文ｃ１’が第１暗号文ｃ１と同じ値でない限り共有鍵Ｋを出力しないようにしたので、復号エラーが発生した場合、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できるようになった。

【０２０９】

＜変形例＞

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。実施の形態１におけるのと同様の変形を施すことができるのはもちろんであるが、以下のような場合も本発明に含まれる。

【０２１０】

（１）暗号化部１１４ｂで行われる乱数値ｕから乱数多項式ｒへの変換方法は、この方法に限られずｕからｒが一意に求まれば他の変換方法でもよい。例えば、乱数値ｕを多項式に対応させる関数もしくは関数値テーブルを用いて変換してもよい。

【０２１１】

（２）暗号化部１１４ｂ、復号化部１２３ｂで用いる公開鍵暗号は、暗号化部１１４ｂにおいて、検証値ａを公開鍵と乱数値ｕを用いて暗号化して第１暗号文ｃ１を生成し、復号化部１２３ｂにおいて、第１暗号文ｃ１を秘密鍵で復号して、検証値ａと等しい復号検証値ａ’を生成できればよい。従って、暗号化部１１４ｂ、復号化部１２３ｂで用いる公開鍵暗号は、ＮＴＲＵ暗号以外に、乱数を用いる公開鍵暗号ならばどんな暗号でも利用できる。

【０２１２】

例えば、ＥｌＧａｍａｌ暗号ならば、ｈ、ｆをそれぞれＥｌＧａｍａｌ暗号の公開鍵、秘密鍵とし、暗号化部１１４ｂにおいて、ａをｈと乱数値ｕを用いて暗号化してｃ１を生成し、復号化部１２３ｂにおいて、ｃ１をｆを用いて復号してａ’を生成すればよい。

【０２１３】

（３）乱数値ｕは、第１関数部１１３ｂ及び第２関数部１２６ｂで生成される以外にも、暗号装置１１０ｂと復号装置１２０ｂとで同じ値を得られれば、他の生成方法でもよい。

【０２１４】

例えば、任意の関数Ｆｕｎｃに対し、ｕ＝Ｆｕｎｃ（ｓ）として暗号装置１１０ｂと復号装置１２０ｂとで同じ値を得られるようにしてもよい。すなわち、

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ、Ｋを生成する。

【０２１５】

・Ｆｕｎｃ（ｓ）を生成し、ｕ＝Ｆｕｎｃ（ｓ）とする。

としてもよい。

【０２１６】

（４）さらに、乱数値ｕは、第１関数部１１３ｂ及び第２関数部１２６ｂで生成される以外にも、暗号装置１１０ｂと復号装置１２０ｂとで同じ値を得られればよいため、暗号装置１１０ｂが乱数値ｕを復号装置１２０ｂに直接送信してもよい。

【０２１７】

すなわち、以下のように、暗号文Ｃと乱数値ｕを復号装置１２０ｂに送信してもよい。また、乱数値ｕは暗号化して送信されてもよい。

【０２１８】

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ、Ｋを生成する。

【０２１９】

・乱数値ｕは、別途、暗号装置１１０ｂから１２０ｂへ送信される。

【０２２０】

（５）さらに、乱数値ｕは、暗号装置１１０ｂと復号装置１２０ｂとで同じ値を得られればよいため、乱数値ｕの部分情報を第１関数部１１３ｂ及び第２関数部１２６ｂで生成し、乱数値ｕの残りの部分情報を暗号装置１１０ｂから復号装置１２０ｂに直接送信してもよい。

【０２２１】

例えば、以下のように、暗号文Ｃと乱数値ｕ２を復号装置１２０ｂに送信してもよい。また、乱数値ｕ２は暗号化して送信されてもよい。

【０２２２】

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ、Ｋ、ｕ１を生成する。

【０２２３】

・乱数値ｕ２は、別途、暗号装置１１０ｂから１２０ｂへ送信される。

【０２２４】

・乱数値ｕは、ｕ＝ｕ１　ｘｏｒ　ｕ２から生成される。

【０２２５】

（６）復号装置１２０ｂは、第１暗号文ｃ１が第２関数部１２６ｂで得られる検証値ａ’’の暗号文かどうかチェックを行い、ｃ１がａ’’の暗号文であるときに共有鍵Ｋ’を用いて共通鍵暗号文Ｃｉを復号しているが、このチェックは、第１暗号文ｃ１が復号検証値ａ’の暗号文かどうかのチェックでもよい。

【０２２６】

（７）また、復号装置１２０ｂは、第１暗号文ｃ１が第２関数部１２６ｂで得られる検証値ａ’’の暗号文かどうかチェックを行い、ｃ１がａ’’の暗号文であるときに共有鍵Ｋ’を用いて共通鍵暗号文Ｃｉを復号しているが、このチェックは、比較部１２７ｂにおいて、復号化部１２３ｂが復号したａ’の値と第２関数部１２６ｂが生成したａ’’の値が等しいかどうかのチェックでもよい。

【０２２７】

（８）なお、復号エラー発生により暗号装置１１０ｂと復号装置１２０ｂとの間で異なる鍵が導出されるのを防止するため、第１再暗号文ｃ１’が第１暗号文ｃ１と同じ値かどうかを検証して共有鍵Ｋ’を出力する代わりに、暗号装置１１０ｂが乱数ｓ、検証値ａ、乱数値ｕ、共有鍵Ｋのいずれかのハッシュ関数値を生成し、復号装置１２０ｂがこのハッシュ関数値を検証して共有鍵Ｋ’を出力するか否かを決定してもよいし、安全性を高めるために、特許文献１に開示されている方法を用いてもよい。すなわち、実施の形態１の変形例（８）を適用してもよい。

【０２２８】

（９）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【０２２９】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、半導体メモリ、ハードディスクドライブ、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ等、に記録したものとしてもよい。

【０２３０】

（１０）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０２３１】

【発明の効果】

以上に説明したように、本発明は、従来システムにおける問題点を鑑みて行われたもので、暗号システムにおいて、ＮＴＲＵ暗号を適用できる新しい鍵カプセル化メカニズムを構成することで、暗号装置と復号装置との間で異なる鍵が導出されるのを防止でき、鍵カプセル化メカニズムにより導出される鍵を用いた送信装置から受信装置への確実な暗号化通信ができるようになった。

【０２３２】

以上により、従来技術では達成できなかった暗号システムを提供することができ、その価値は大きい。

【図面の簡単な説明】

【図１】

本発明の実施の形態１における暗号システム１の構成を示す図

【図２】

本発明の実施の形態１における暗号装置１１０の構成を示す図

【図３】

本発明の実施の形態１における暗号装置１１０の処理の流れ図

【図４】

本発明の実施の形態１における復号装置１２０の構成を示す図

【図５】

本発明の実施の形態１における復号装置１２０の処理の流れ図

【図６】

本発明の実施の形態１における暗号装置１１０の変形例の構成を示す図

【図７】

本発明の実施の形態１における復号装置１２０の変形例の構成を示す図

【図８】

本発明の実施の形態２における暗号システム２の構成を示す図

【図９】

本発明の実施の形態２における暗号装置１１０ｂの構成を示す図

【図１０】

本発明の実施の形態２における復号装置１２０ｂの構成を示す図

【符号の説明】

１，２　暗号システム

１１０，１１０ａ　暗号装置

１１１　公開鍵入力部

１１２，１１２ｂ　乱数生成部

１１３，１１３ｂ　第１関数部

１１４，１１４ｂ　暗号化部

１１６　乱数マスク部

１１７，１１７ｂ　送信部

１１８　共通鍵暗号部

１１９　共通鍵暗号文送信部

１２０，１２０ｂ　復号装置

１２１　秘密鍵入力部

１２２，１２２ｂ　受信部

１２３，１２３ｂ　復号化部

１２５　乱数マスク除去部

１２６，１２６ｂ　第２関数部

１２７，１２７ｂ　比較部

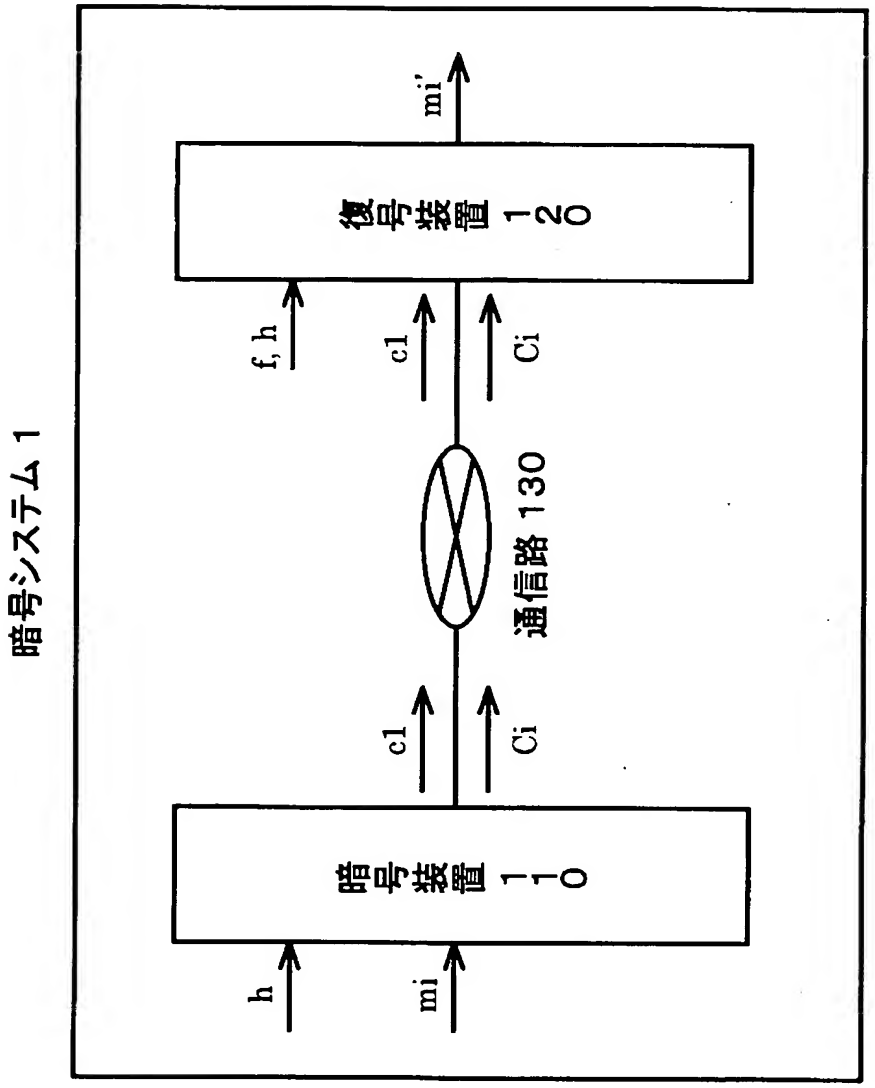
１２８　共通鍵復号部

１２９　共通鍵暗号文受信部

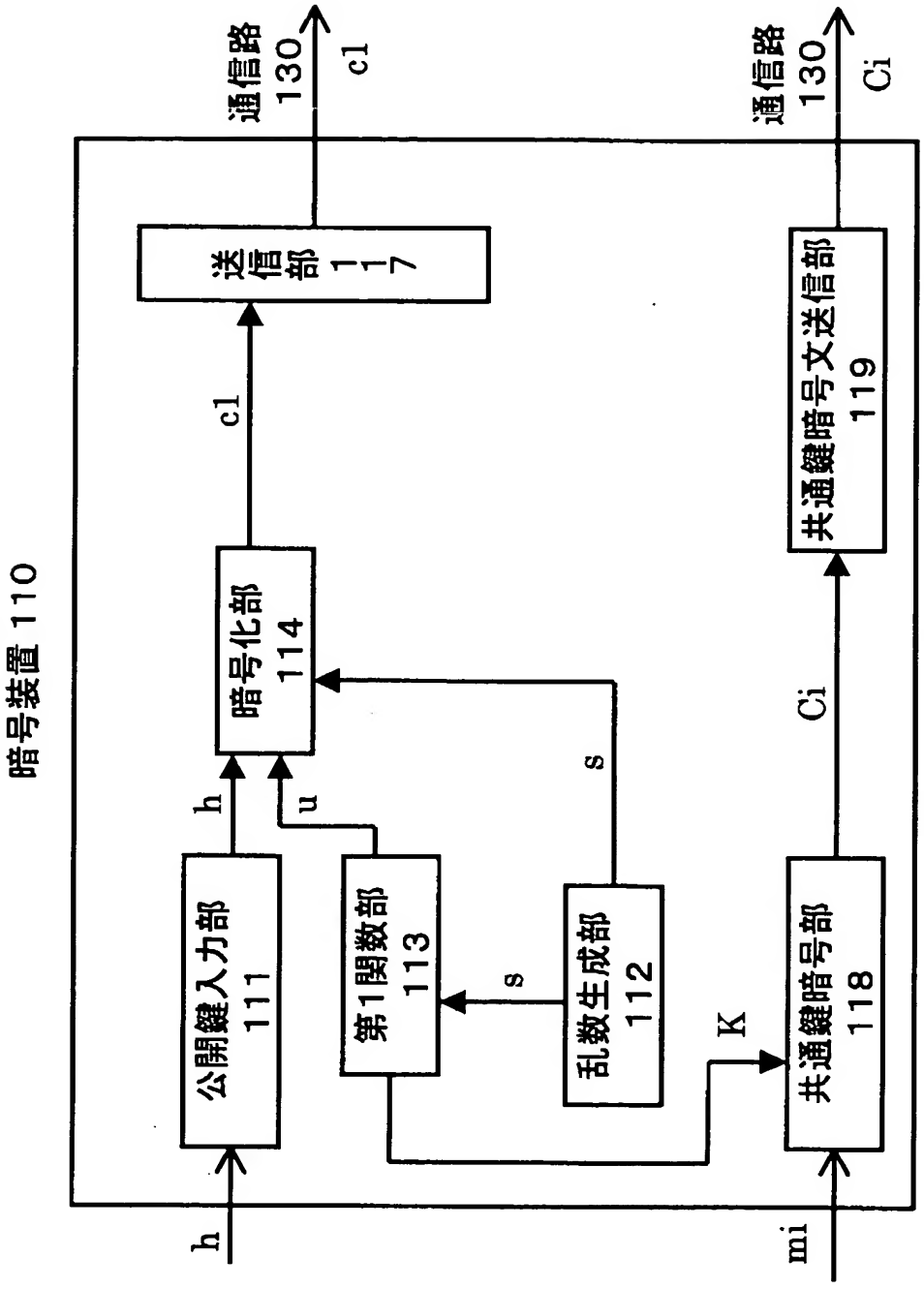
１３０　通信路

【書類名】　図面

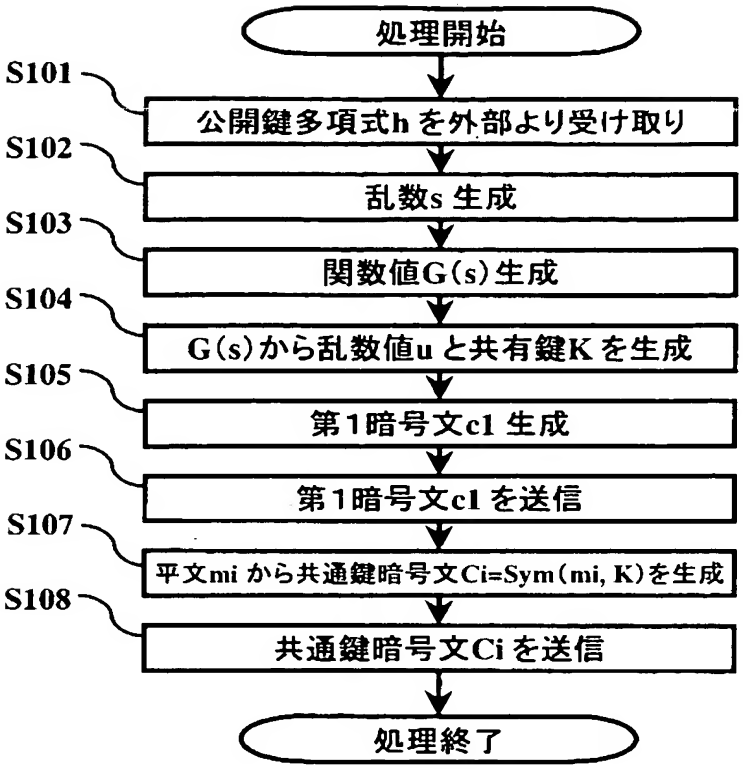
【図１】



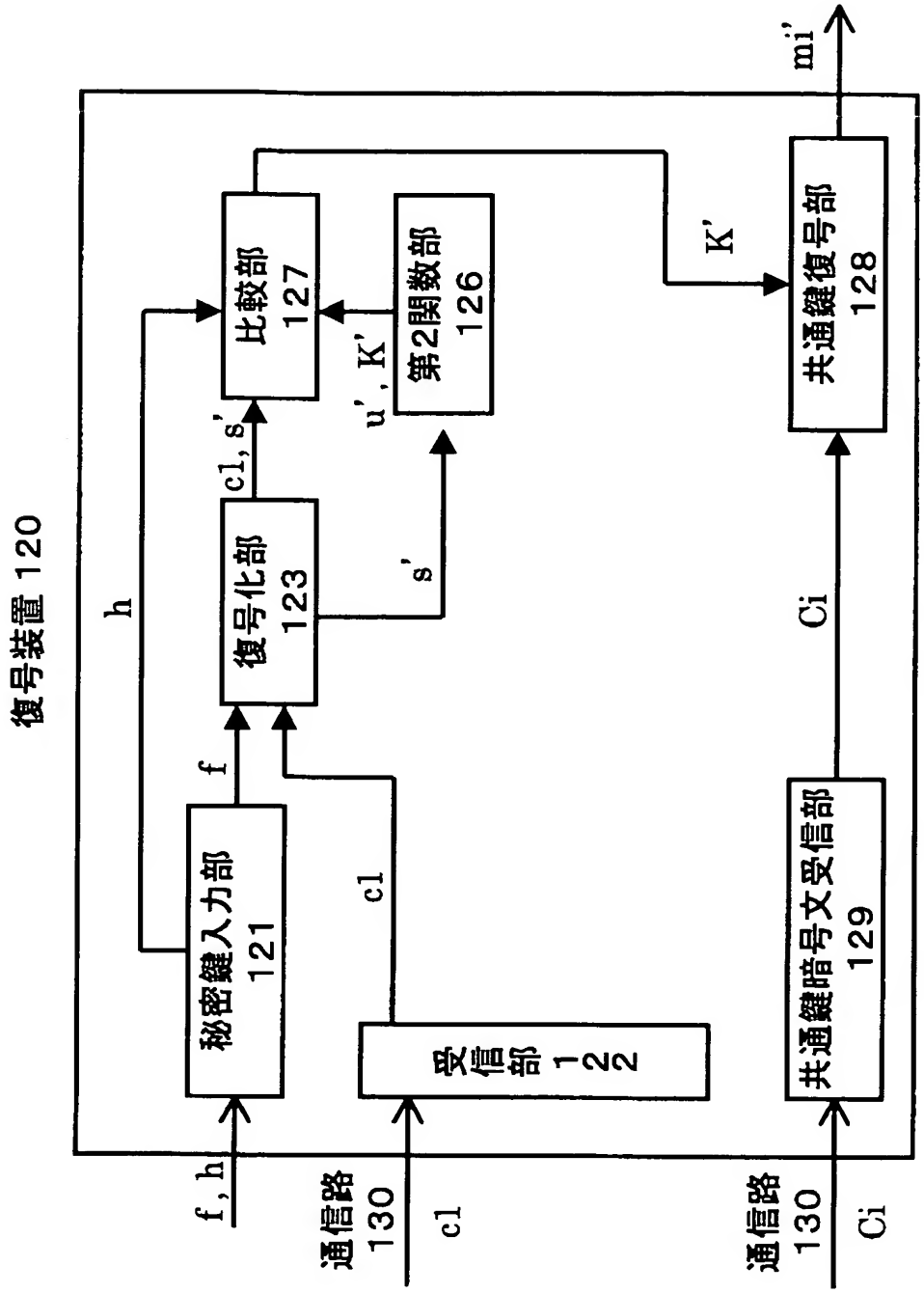
【図２】


暗号装置 110
通信路 130
c1
通信路 130
Ci
送信部 117
c1
共通鍵暗号文送信部 119
暗号化部 114
Ci
h
u
s
公開鍵入力部 111
第1関数部 113
乱数生成部 112
共通鍵暗号部 118
s
K
h
mi

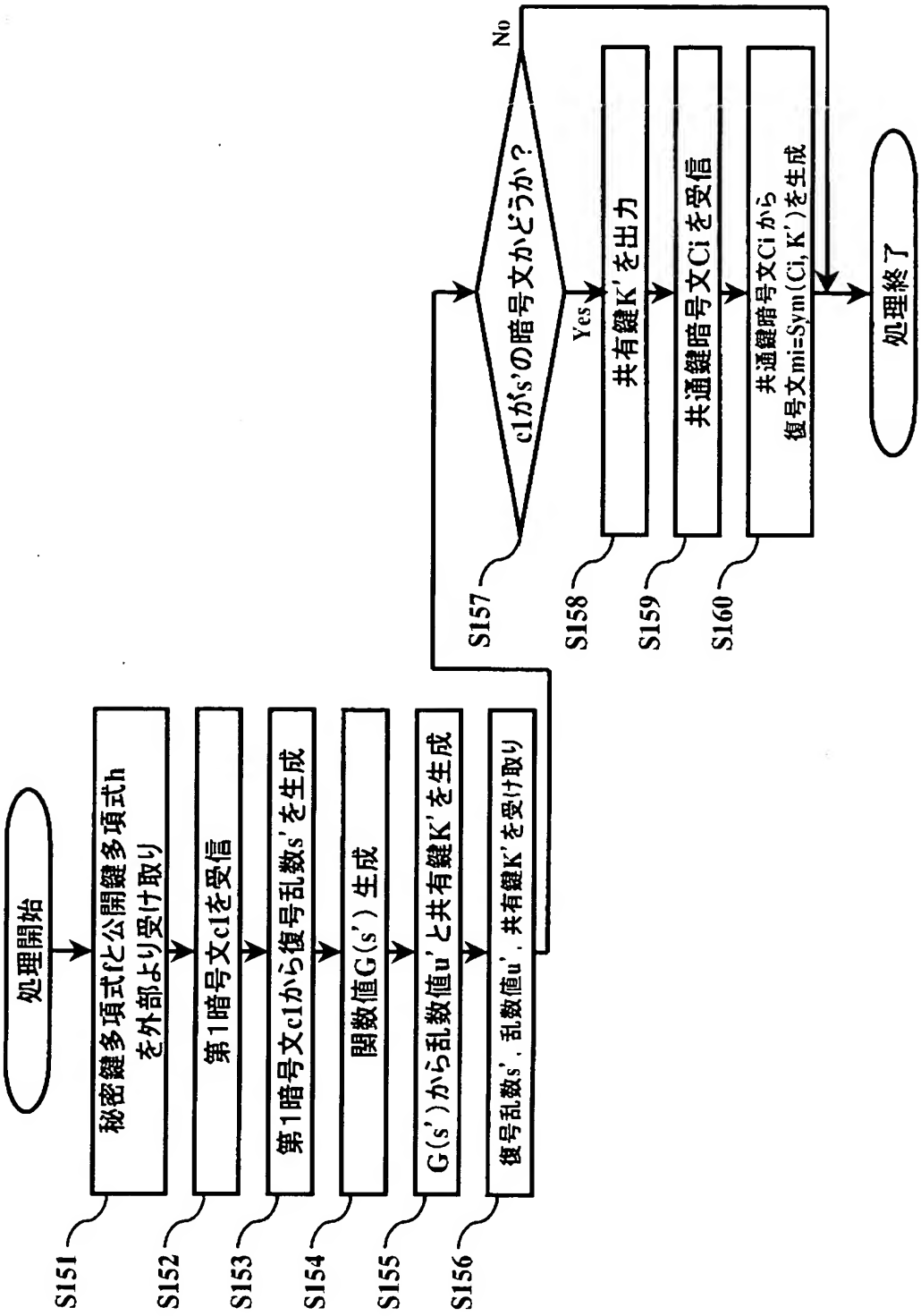
【図３】


処理開始
S101
公開鍵多項式h を外部より受け取り
S102
乱数s 生成
S103
関数値G(s)生成
S104
G(s)から乱数値u と共有鍵K を生成
S105
第1暗号文c1 生成
S106
第1暗号文c1 を送信
S107
平文mi から共通鍵暗号文Ci=Sym(mi, K)を生成
S108
共通鍵暗号文Ci を送信
処理終了

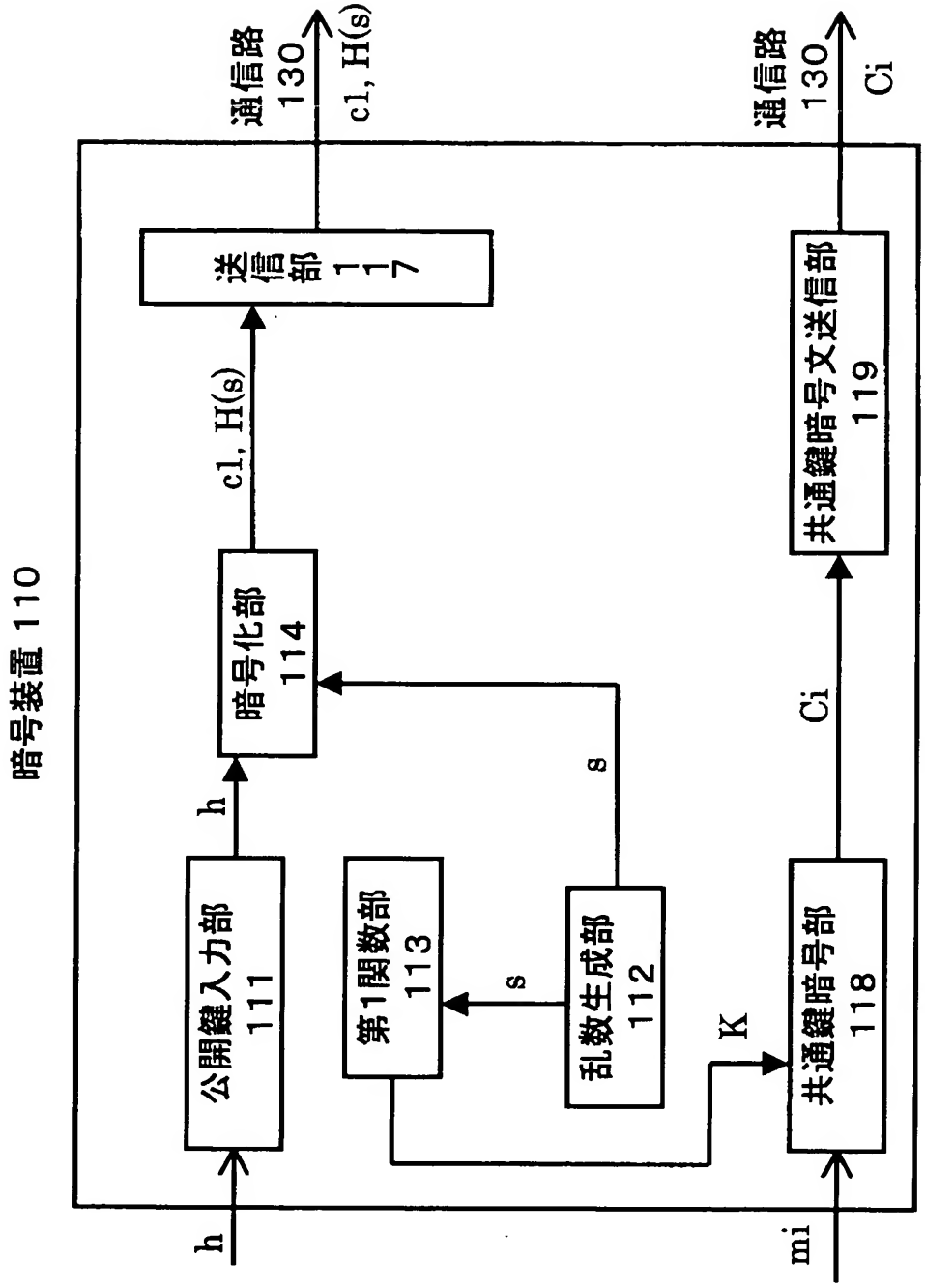
【図４】


復号装置 120
秘密鍵入力部 121
受信部 122
復号化部 123
比較部 127
第2関数部 126
共通鍵復号部 128
共通鍵暗号文受信部 129
通信路 130
通信路 130
f, h
c1
Ci
f
h
c1
s'
c1, s'
u', K'
K'
mi'

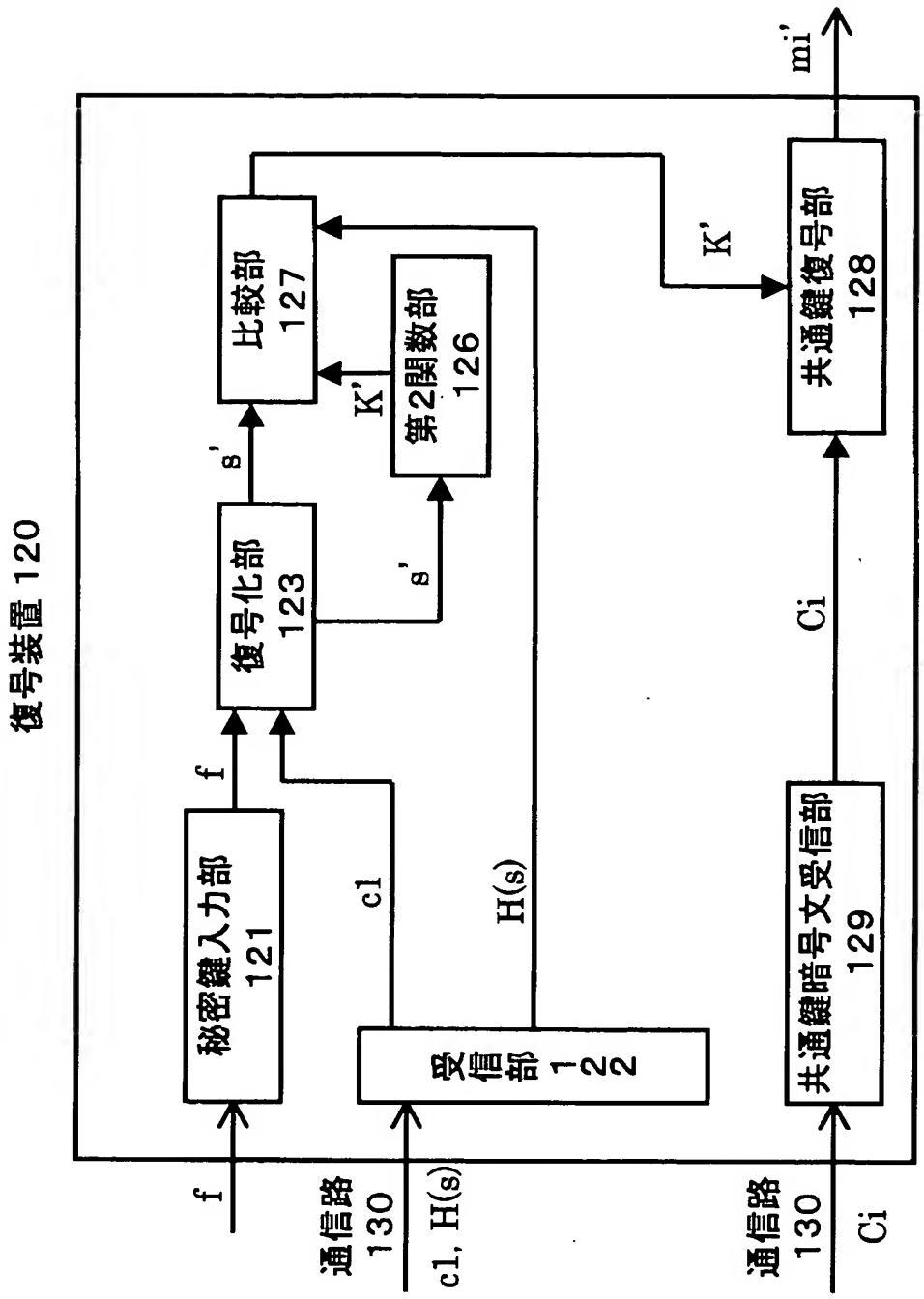
【図５】


処理開始
秘密鍵多項式fと公開鍵多項式h
を外部より受け取り
第1暗号文c1を受信
第1暗号文c1から復号乱数s'を生成
関数値G(s')生成
G(s')から乱数値u'と共有鍵K'を生成
復号乱数s', 乱数値u', 共有鍵K'を受け取り
c1がs'の暗号文かどうか？
No
Yes
共有鍵K'を出力
共通鍵暗号文Ciを受信
共通鍵暗号文Ciから
復号文mi=Sym(Ci, K')を生成
処理終了
S151
S152
S153
S154
S155
S156
S157
S158
S159
S160

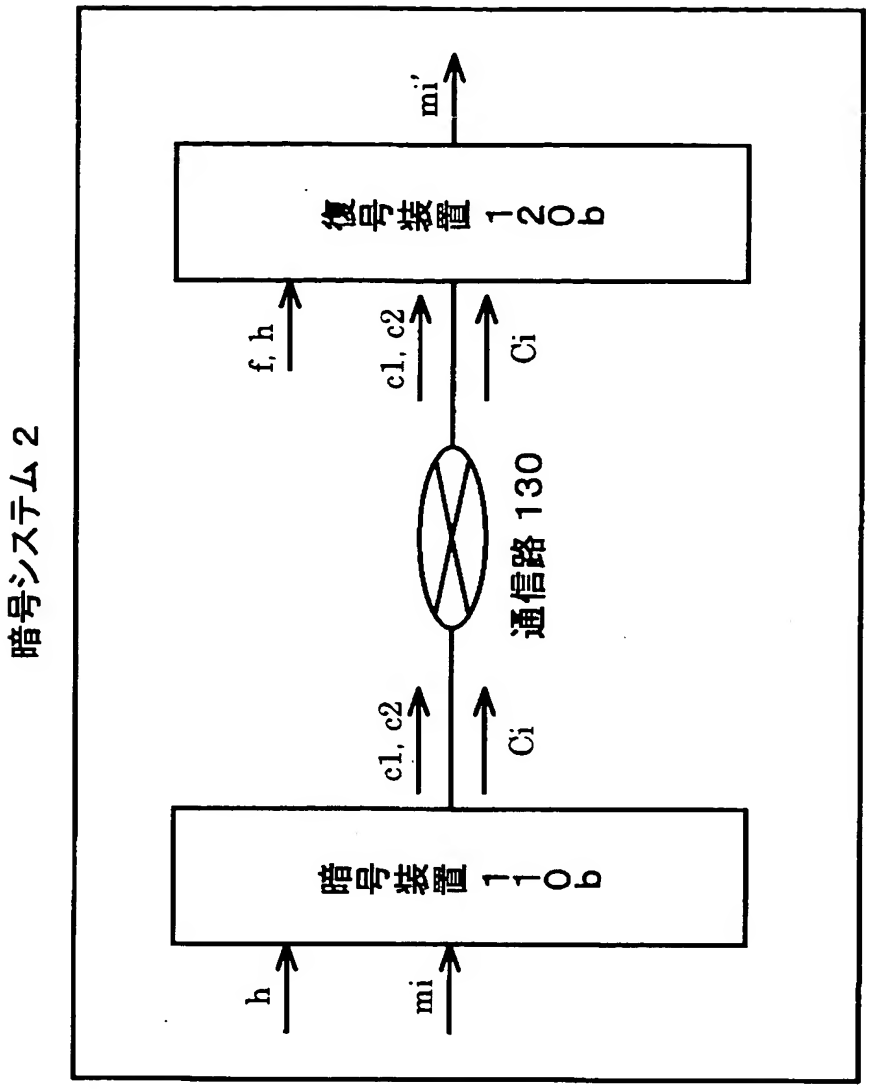
【図６】


暗号装置 110
通信路 130
c1, H(s)
送信部 117
c1, H(s)
暗号化部 114
h
公開鍵入力部 111
h
第1関数部 113
s
乱数生成部 112
s
K
共通鍵暗号部 118
mi
Ci
共通鍵暗号文送信部 119
Ci
通信路 130

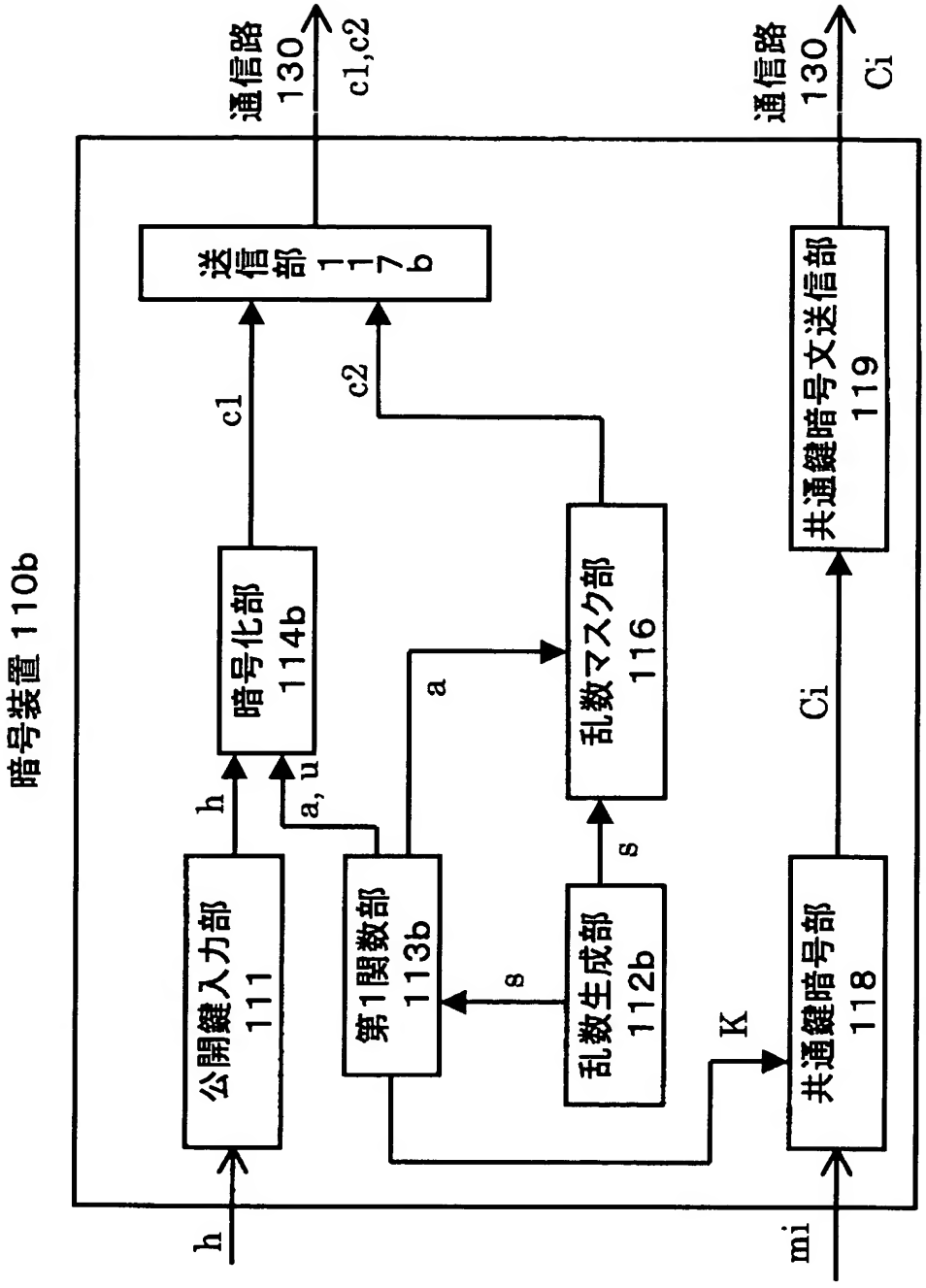
【図７】


復号装置 120
秘密鍵入力部 121
復号化部 123
第2関数部 126
比較部 127
共通鍵復号部 128
共通鍵暗号文受信部 129
受信部 122
f
s'
K'
c1
H(s)
Ci
mi'
通信路 130
c1, H(s)
通信路 130
Ci

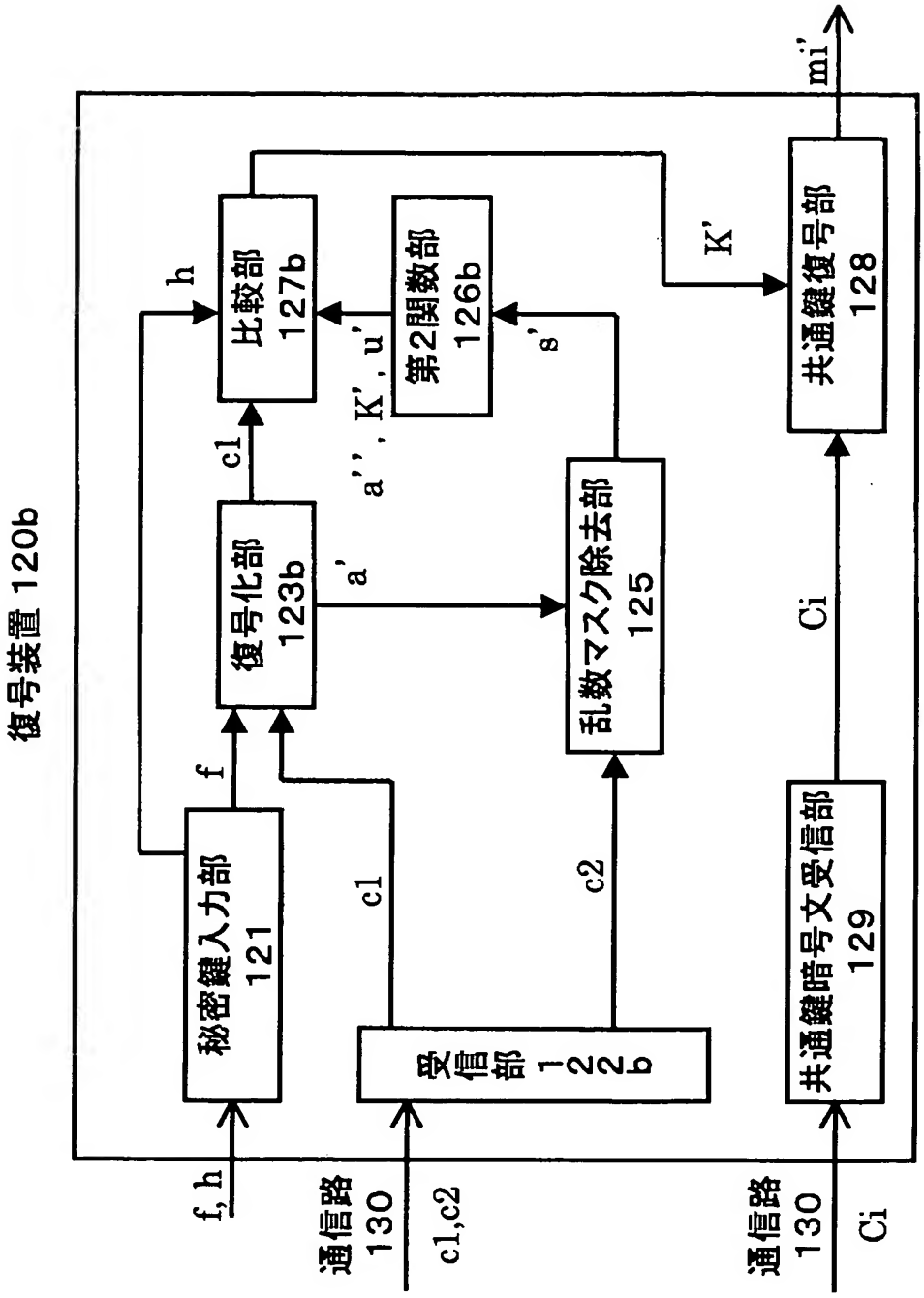
【図８】



【図９】


暗号装置 110b
通信路 130
c1,c2
通信路 130
Ci
送信部 117b
c1
c2
暗号化部 114b
乱数マスク部 116
共通鍵暗号文送信部 119
h
a, u
a
Ci
公開鍵入力部 111
第1関数部 113b
乱数生成部 112b
s
s
K
共通鍵暗号部 118
h
mi

【図１０】


復号装置 120b
秘密鍵入力部 121
復号化部 123b
比較部 127b
第2関数部 126b
乱数マスク除去部 125
共通鍵復号部 128
共通鍵暗号文受信部 129
受信部 122b
f
h
c1
c2
a'
a'', K', u'
s'
K'
Ci
mi'
f, h
通信路 130
c1,c2
通信路 130
Ci

【書類名】　要約書

【要約】

【課題】　ＮＴＲＵ暗号を用いて新しい鍵カプセル化メカニズムを構成し、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できる暗号システム、暗号装置、復号装置を提供することを第１の目的とする。

【解決手段】　本発明は、秘密数データを生成する秘密数データ生成手段と、前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して暗号化共有鍵データを生成する第１の暗号化手段とを備えることを特徴とする。

【選択図】　図２

特願２００２－３５１０６３

# 出　願　人　履　歴　情　報

識別番号　　［０００００５８２１］

１．変更年月日　　１９９０年　８月２８日
［変更理由］　　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社